



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000137774 A**(43) Date of publication of application: **16.05.00**

(51) Int. Cl. **G06K 17/00**
G06K 19/07
G07B 15/00
G09C 1/00
H04B 5/02
H04L 9/32

(21) Application number: **11218020**(22) Date of filing: **30.07.99**(30) Priority: **31.07.98 JP 10217236**(71) Applicant: **MATSUSHITA ELECTRONICS
INDUSTRY CORP**(72) Inventor: **AZUMA MASAMICHI**

(54) **PORTABLE BODY USED FOR TWO USES,
COMMUNICATION SYSTEM, COMMUNICATION
METHOD, TERMINAL DEVICE, AND COMPUTER-
READABLE RECORDING MEDIUM WHERE
PROGRAM IS RECORDED**

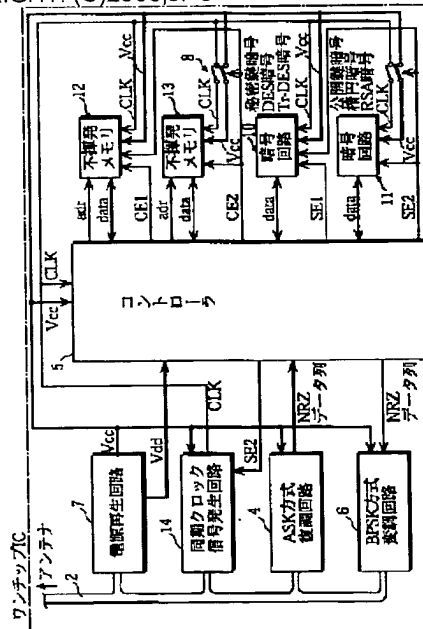
this nonvolatile memory 13 is carried out by using the
ciphering circuit 11 to complete the protection of the
individual information.

COPYRIGHT: (C)2000,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a portable body which is used for two purposes such as an account settlement use and a ticket examination use without making electric contact by a connector.

SOLUTION: The integrated device of an IC card is equipped with a nonvolatile memory 12 which is accessed when a terminal device is approached up to several to ten of cm and a ciphering circuit 10 which performs two-way authentication cooperatively with a 1st terminal device. In addition, the integrated device is equipped with a nonvolatile memory 13 which is accessed only when the terminal device is approached up to 0 to 5 mm and large electric power is supplied from an antenna and a ciphering circuit 11 which performs two-way authentication cooperatively with the 1st terminal device. Individual information which should be kept highly secret is stored in this nonvolatile memory 13 and the two-way authentication at the time of access to



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-137774
(P2000-137774A)

(43) 公開日 平成12年5月16日 (2000.5.16)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 K 17/00		G 0 6 K 17/00	F
		G 0 7 B 15/00	5 0 1
G 0 7 B 15/00	5 0 1	G 0 9 C 1/00	6 6 0 A
G 0 9 C 1/00	6 6 0	H 0 4 B 5/02	
H 0 4 B 5/02		G 0 6 K 19/00	H

審査請求 有 請求項の数15 O L (全 28 頁) 最終頁に続く

(21) 出願番号 特願平11-218020
(22) 出願日 平成11年7月30日 (1999.7.30)
(31) 優先権主張番号 特願平10-217236
(32) 優先日 平成10年7月31日 (1998.7.31)
(33) 優先権主張国 日本 (J P)

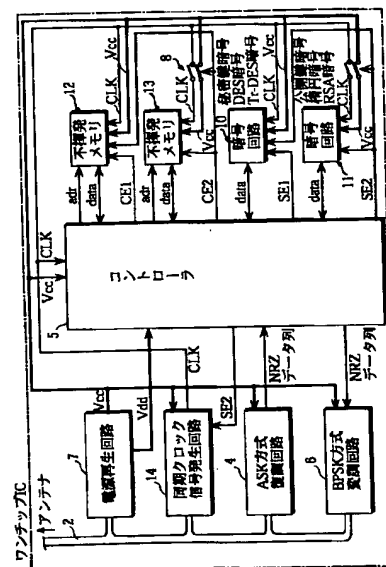
(71) 出願人 000005843
松下電子工業株式会社
大阪府高槻市幸町1番1号
(72) 発明者 吾妻 正道
大阪府高槻市幸町1番1号 松下電子工業
株式会社内
(74) 代理人 100090446
弁理士 中島 司朗 (外1名)

(54) 【発明の名称】 2つの用途で用いられる可搬体、通信システム、通信方式、端末装置、プログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 コネクタによる電気的接触を行わずに、決済用途や改札用途等、2つの用途に用いることができる可搬体を提供する。

【解決手段】 ICカード1における集積デバイスには、端末装置に数cm〜10cmまで接近した場合、アクセスされる不揮発メモリ12と、第1端末装置と協調して双方向認証を行う暗号回路10とが備えられている。これと共に、集積デバイスには、端末装置に0mm〜5mmまで接近し、アンテナからより大きな電力が供給された場合のみアクセスされる不揮発メモリ13と、第1端末装置と協調して双方向認証を行う暗号回路11とが備えられている。この不揮発メモリ13に機密性が強く求められる個人情報情報を記憶させ、この不揮発メモリ13をアクセスする際の双方向認証を、暗号回路11を用いて行えば、個人情報の保護は万全となる。



【特許請求の範囲】

【請求項1】 2つの用途で用いられる可搬体であっ

て、

可搬体には、集積デバイスが設けられており、

前記集積デバイスは、

電波送信を行っている端末装置に可搬体が接近すると、

可搬体が何れの用途に用いられるかを、端末装置からの電波に基づいて特定する特定手段と、

可搬体が第1の用途で用いられる場合には、第1の処理を行い、可搬体が第2の用途で用いられる場合には、第2の処理を行う処理手段と、

第1の用途で用いられる場合、第2の用途で用いられる場合の双方において、端末装置と無線通信を行うことにより、端末装置と処理手段との間で非接触式の入出力を行う通信手段とを備えることを特徴とする可搬体。

【請求項2】 前記特定手段は、

可搬体が電波送信を行っている端末装置に接近した場合、端末装置と可搬体との距離が第1所定距離未満であれば、可搬体が第2の用途に用いられると判定し、端末装置と可搬体との距離が第2所定距離以上第3所定距離以内であれば、可搬体が第1の用途に用いられると判定する判定部を備えることを特徴とする請求項1記載の可搬体。

【請求項3】 前記集積デバイスは、

前記端末装置から、電波にて電力供給を受けており、集積デバイスが端末装置から供給を受ける電力は、端末装置との距離に応じて増減し、

前記特定手段は、

可搬体が電波送信を行っている端末装置に接近した際、アンテナが電波を受信した際の受信電圧と所定の閾値とを比較する比較部を備え、

前記判定部は、

前記電波を受信した際の受信電圧が閾値を上回る場合、端末装置と可搬体との距離が第1所定距離未満であると判定し、

前記電波を受信した際の受信電圧が閾値を下回る場合、端末装置と可搬体との距離が第2所定距離以上第3所定距離以内であると判定することを特徴とする請求項2記載の可搬体。

【請求項4】 前記端末装置には、

第1所定電力未満の電波を出力する第1端末装置と、電磁シールドがなされた筐体内部にアンテナを有しており、この筐体内部において、第1所定電力の倍以上の第2所定電力を有する電波を可搬体に出力する第2端末装置とがあり、

前記閾値は、

前記第2所定距離以上第3所定距離以内の範囲において、第1所定電力の電波を受信した際の受信電力と、当該アンテナから第1所定距離未満の範囲において、第2所定電力の電波を受信した際の受信電力とに基づいて、

設定されていることを特徴とする請求項3記載の可搬体。

【請求項5】 第2の用途は、第1の用途より高い機密性が求められるものであり、

第1処理は、第1暗号鍵を用いてデータを暗号化する暗号化処理、第1暗号鍵を用いて暗号化されたデータを復号する復号化処理、端末装置からの認証処理に対して第1暗号鍵を用いて自身の正当性を証明する証明処理、第1暗号鍵を用いて端末装置の正当性を認証する認証処理の何れか1つを含んでいて、

第2処理は、前記第1暗号鍵より安全性が高い第2暗号鍵を用いて、データを暗号化する暗号化処理、第2暗号鍵を用いて暗号化されたデータを復号する復号化処理、端末装置からの認証処理に対して自身の正当性を第2暗号鍵を用いて証明する証明処理、第2暗号鍵を用いて端末装置の正当性を認証する認証処理のうち何れか1つを含んでおり、

第2処理は、第1処理より処理負荷が大きく、前記第2所定電力は、処理手段が第2処理を行う場合に消費される電力に基づいた値に設定されていることを特徴とする請求項4記載の可搬体。

【請求項6】 前記集積デバイスは、

第1の用途においてのみ用いられるデータを記憶する第1領域と、第2の用途のみに用いられるデータを記憶する第2領域を含む記憶手段を含み、

前記通信手段は、

端末装置から無線にて発行されたコマンドを受信すると共に、端末装置に出力すべきデータを無線にて端末装置に送信する送受信部を備え、

前記処理手段は、

特定手段により何れかの用途が特定された場合、第1領域及び第2領域のうち、特定された用途に割り当てられている領域のみのアクセスを許可し、それ以外の領域のアクセスを禁止するアクセス管理部と、

前記送受信部が受信したコマンドを解読する解読部と、

前記解読部による解読結果がリードコマンドである場合、リードコマンドにて指示されているデータを第1領域又は第2領域から読み出して、送受信部に送信させ、解読結果がライトコマンドである場合、ライトコマンドにて指示されたデータを第1領域又は第2領域に書き込むメモリアクセス部とを含むことを特徴とする請求項5記載の可搬体。

【請求項7】 前記集積デバイスは、

第1端末装置から第1所定電力が供給された場合、受信信号における搬送波の周波数に基づいた第1周波数を有する同期クロック信号を処理手段に供給すると共に、第2端末装置から第2所定電力が供給された場合、第1周波数より高い第2周波数を有する同期クロック信号を処理手段に供給する同期クロック信号発生部を備えることを特徴とする請求項4記載の可搬体。

【請求項 8】 前記端末装置には、

第 1 ポーリングコマンドが変調された電波を出力することにより、ポーリングを行っている第 1 端末装置と、
第 2 ポーリングコマンドが変調された電波を出力することにより、ポーリングを行っている第 2 端末装置とがあり、

前記特定手段は、

可搬体が運搬されて、電波送信にてポーリングを行っている第 1 端末装置、第 2 端末装置の何れかに接近すれば、送信されている電波に変調されているコマンドに第 1 1 ポーリングコマンド、第 2 ポーリングコマンドの何れが含まれているかを判定する判定部を備え、

第 1 ポーリングコマンドが含まれていると判定された場合、可搬体が第 1 の用途に用いられると特定し、第 2 ポーリングコマンドが含まれていると判定された場合、可搬体が第 2 の用途に用いられると特定することを特徴とする請求項 1 記載の可搬体。

【請求項 9】 可搬体と通信を行う端末装置であって、可搬体には、集積デバイスが設けられており、

前記集積デバイスは、

所定の処理を行う第 1 モード、第 1 モードよりも機密性が高い処理を行う第 2 モードの何れかに設定され、

端末装置は、

その内部にアンテナを有しており、アンテナから放射された電波が一定値以上装置外部に放射されないように電磁シールドがなされている筐体と、

この筐体内部に可搬体が挿入されると、集積デバイスを第 2 モードに設定させてから、アンテナに電波を放射させることにより、集積デバイスとの通信を行う通信手段とを備えることを特徴とする端末装置。

【請求項 10】 前記端末装置は、

この筐体内部に可搬体が挿入されると、可搬体の正当性を物理的に示す物理情報を可搬体から読み取る第 1 読み取り部と、所有者本人の正当性を示す所有者情報の入力を所有者から受け付ける受付部と、所有者本人の肉体的な特徴を示すバイオ情報を所有者から読み取る第 2 読み取り部のうち、少なくとも 1 つを備えており、

前記通信手段は、

第 1 読み取り部が読み取った物理個人情報、受付部が受け付けた所有者情報、第 2 読み取り部が読み取ったバイオ情報のうち、少なくとも 1 つを用いて、所有者又は可搬体の正当性を確認してから、集積デバイスの状態を第 2 モードに設定させることを特徴とする請求項 9 記載の端末装置。

【請求項 11】 可搬体、第 1 端末装置、第 2 端末装置からなる通信システムであって、

可搬体には、所定の処理を行う第 1 モード、第 1 モードよりも機密性が高い処理を行う第 2 モードの何れかに設定される集積デバイスが設けられており、

前記第 1 端末装置は、

可搬体が接近すれば、集積デバイスを第 1 モードに設定させてから、可搬体と電波の送受信を行うことにより、集積デバイスとの間で非接触式の入出力を行う第 1 通信手段を備え、

第 2 端末装置は、

その内部にアンテナを有しており、アンテナから放射された電波が一定値以上装置外部に放射されないように電磁シールドがなされている筐体と、

この筐体内部に可搬体が挿入されると、集積デバイスを第 2 モードに設定させてから、アンテナに電波を放射させて可搬体と電波の送受信を行うことにより、集積デバイスとの間で非接触式の入出力を行う第 2 通信手段を備えることを特徴とする通信システム。

【請求項 12】 可搬体、第 1 端末装置、第 2 端末装置からなる通信システムにおける通信方式であって、可搬体には、所定の処理を行う第 1 モード、第 1 モードよりも機密性が高い処理を行う第 2 モードの何れかに設定される集積デバイスが設けられており、

前記第 1 端末装置は、

可搬体が接近すれば、集積デバイスを第 1 モードに設定させてから、可搬体と電波の送受信を行うことにより、集積デバイスとの間で非接触式の入出力を行い、

第 2 端末装置は、

その内部にアンテナを有しており、アンテナから放射された電波が一定値以上装置外部に放射されないように電磁シールドがなされている筐体を有しており、

この筐体内部に可搬体が挿入されると、集積デバイスを第 2 モードに設定させてから、アンテナに電波を放射させて可搬体と電波の送受信を行うことにより、集積デバイスとの間で非接触式の入出力を行うことを特徴とする通信方式。

【請求項 13】 可搬体とデータの入出力を行う端末装置であって、

可搬体には、所定の処理を行う第 1 モード、第 1 モードよりも機密性が高い処理を行う第 2 モードの何れかに設定され、集積デバイスが設けられており、

前記端末装置は、

端末装置から第 2 所定距離以上第 3 所定距離以内に可搬体が接近すれば、集積デバイスを第 1 モードに設定させてから、可搬体と電波の送受信を行うことにより、集積デバイスとの間で非接触式の入出力を行う第 1 通信手段と、

端末装置から第 1 所定距離未満内に可搬体が接近すれば、集積デバイスを第 2 モードに設定させてから、可搬体と電波の送受信を行うことにより、集積デバイスとの間で非接触式の入出力を行う第 2 通信手段とを備えることを特徴とする端末装置。

【請求項 14】 可搬体とデータの入出力を行うプログラムが記録されたコンピュータ読取可能な記録媒体であ

って、

可搬体には、所定の処理を行う第1モード、第1モードよりも機密性が高い処理を行う第2モードの何れかに設定され、集積デバイスが設けられており、前記プログラムは、

端末装置から第2所定距離以上第3所定距離以内に可搬体が接近すれば、集積デバイスを第1モードに設定させてから、可搬体と電波の送受信を行うことにより、集積デバイスとの間で非接触式の入出力を行う第1ステップと、

端末装置から第1所定距離未満内に可搬体が接近すれば、集積デバイスを第2モードに設定させてから、可搬体と電波の送受信を行うことにより、集積デバイスとの間で非接触式の入出力を行う第2ステップとをコンピュータに実行させることを特徴とするコンピュータ読取可能な記録媒体。

【請求項15】 可搬体と端末装置との間の通信方式であって、

可搬体には、所定の処理を行う第1モード、第1モードよりも機密性が高い処理を行う第2モードの何れかに設定される集積デバイスが設けられており、

前記端末装置は、

端末装置から第2所定距離以上第3所定距離以内に可搬体が接近すれば、集積デバイスを第1モードに設定させてから、可搬体と電波の送受信を行うことにより、集積デバイスとの間で非接触式の入出力を行い、

端末装置から第1所定距離未満内に可搬体が接近すれば、集積デバイスを第2モードに設定させてから、可搬体と電波の送受信を行うことにより、集積デバイスとの間で非接触式の入出力を行うことを特徴とする通信方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、端末装置との間で無線で処理を行うICカード等、集積デバイスが実装された可搬体、通信システム、通信方式、端末装置、プログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】自治体、交通機関、金融機関、医療機関等は、ICカードを用いた個人情報の管理に強い関心を抱いている。ICカードとは、不揮発メモリ、プロセッサ、認証回路等の集積デバイスをカードに実装したものであり、このワンチップICに個人情報を記憶させると、所有者は、ICカードを肌身離さず常時携帯しておくことができ、必要に応じて、いつでもこのICカードに記憶されている個人情報を閲覧することができる。更にICカードには、認証回路を集積させることができるので、この認証回路を用いれば、それに記憶されている個人情報の不正な読み出しが困難になり、磁気的に個人情報を記録した磁気カード等と比較して、個人情報の守秘の万全化

が図ることができる。このようなICカードの仕様は、IS0規格にすでに規定されている内容、あるいはこれから規定されようとしている内容に準拠することになる。ここでISO規格には、遠隔型と呼ばれるICカードがISO14443に規定されており、密接型と呼ばれるICカードがISO1536に規定されている。

【0003】このうち、遠隔型のICカードとは、端末装置から電波で電力供給を受けながら、集積デバイスが稼働するタイプであり、定期乗車券の検閲や施設の入退出管理等の用途に向いているといわれる。例えば、鉄道の改札に端末装置が設けられており、ICカードを携帯した所有者が、これから列車に搭乗しようとする場合、所有者は、このICカードを端末装置にかざしただけで、端末装置が発する電波によりこのICカードに備えられている集積デバイスが端末装置からの電力供給により稼働する。例えば、このICカードに、この所有者がこの鉄道の定期搭乗者である旨、乗車期間、乗車区間を記憶したメモリ回路と、認証回路とが実装されている場合、改札に設けられた端末装置は、これらメモリ回路及び認証回路と協調して、所有者の信憑性をチェックする。もし、乗車期間や乗車区間に問題が無いなら、端末装置は、所有者をプラットホームに進入させ、乗車期間や乗車区間に問題があるなら、端末装置は、所有者がプラットホームに進入することを拒否する。

【0004】以上のような、ICカードを用いた簡易な定期乗車の検閲が一般に普及すれば、磁気カード式の定期券のように、定期券を定期入れから取り出して改札機を通過させるという手間が不要となるので、定期搭乗者が改札を通過する際の手間が簡略化され、大都市ターミナルでラッシュアワー時に見受けられるような改札口の混雑が解消されと考えられる。

【0005】遠隔型のICカードは、端末装置との間に隔たりがあったとしても、ICカードと端末装置と協調して、上記のような改札業務等、個人情報の処理が行えるので、利便性の面で遠隔型のICカードは優れており、ゆくゆくは、個人情報の管理のためのICカードの仕様は、遠隔型に統合されるのが良いような印象を受ける。しかしながら、現状の遠隔型ICカードは、機密性が強く求められる個人情報を、端末装置と協調処理することに不向きであり、機密性が強く求められる個人情報には、別のタイプのICカードを用いるのが望ましいと考えられている。

【0006】機密性が強く求められる個人情報の処理に遠隔型のICカードが不向きな理由は以下の通りである。即ち、端末装置とICカードとの間で個人情報の送受信が行われている場合、個人情報の送受信中の端末装置に、悪意の第三者が別のICカードを端末装置にかざせば、悪意の第三者は、当該別のICカードに、端末装置とICカードとの間で送受信されている個人情報を記憶させることができる。

【0007】また、端末装置とICカードとの間で個人情報の送受信が行われている場合、そのような個人情報は、端末装置の近辺に設置された他の通信装置が受信することも可能である。その他の通信装置が、悪意の第三者により操作されている場合、個人情報、その悪意の第三者により傍受されたり、また、受信されたデータが不正に改竄されて、端末装置に送信されることも有り得る。つまり、遠隔型のICカードが端末装置との協調処理を行う場合、個人情報は、常に漏洩の危機にさらされているのである。

【0008】このようなことを考えると、遠隔型のICカードに、重要な個人情報を記憶させ、これについての処理を遠隔型のICカードに委ねるのは望ましくない。遠隔型における利便性を維持しつつも、重要な個人情報を記憶させるには、遠隔型の仕様と、接触型の仕様とを兼備したコンビネーション型のICカードを構成することが考えられる。接触型のICカードは、板体から電極部が露出しており（一般に、このような露出した電極部はコネクタと呼ばれる。）、コネクタで端末装置と接続することにより集積デバイスが稼働する。接触型ICカードが端末装置に接続されると、たとえ悪意の第三者が端末装置の近辺に他の通信装置を設置しても、個人情報を傍受することは不可能となる。また端末装置は暗証番号入力等、カード所有者の信憑性を確認することができるので、接触型のICカードは、セキュリティの面において遠隔型より遥かに優れており、金銭の決済用途等に向いているといえる。

【0009】

【発明が解決しようとする課題】しかしながらコンビネーション型のICカードにおけるコネクタは、汚れたり、汗が付着したり、湿度の高い場所に配されたりすると、導電性が悪くなるので、カード所有者はコンビネーション型のICカードを丁寧に取り扱いねばならないという問題点がある。また、手作業でコネクタの挿抜を行う場合は、コネクタが破損しないように、所有者はコネクタの挿抜を慎重に行わねばならないので、所有者は、ICカードを利用する度に神経を擦り減らしてしまう。コンビネーション型のICカードを銀行等の金融機関に取り付けられた現金支払機等に用いる場合に、所有者の各人がコネクタの挿抜に煩わされれば、一人一人がお金の決済を行うのに時間がかかり、現金支払機の利用者が多い銀行決済日等では、現金支払機の前に長蛇の列ができかねない。

【0010】加えて、コンビネーション型のICカードと端末装置との接続を繰り返せば、両者のコネクタが磨耗し、コネクタの接触不良が生じることは避け得ない。このような接触不良の発生により、両者のメンテナンスが絶えず要求されるのであれば、現金支払機を設置する金融機関は、コンビネーション型ICカードの導入を、断念してしまう可能性がある。

10

【0011】本発明の第1の目的は、コネクタによる電氣的接触を行わずに、決済用途や改札用途等、2つの用途に用いることができる可搬体を提供することである。本発明の第2の目的は、決済用途や改札用途等、2つの用途の切り換えを所有者に手軽に行わせることができる可搬体を提供することである。本発明の第3の目的は、負荷が軽い処理が要求される用途と、負荷が重い処理が要求される用途との切り換えが可能な可搬体を提供することである。

10 【0012】

【課題を解決するための手段】上記第1の目的を達成するために本発明に係る可搬体は、電波送信を行っている端末装置に可搬体が接近すると、可搬体が何れの用途に用いられるかを、端末装置からの電波に基づいて特定する特定手段と、可搬体が第1の用途で用いられる場合には、第1の処理を行い、可搬体が第2の用途で用いられる場合には、第2の処理を行う処理手段と、第1の用途で用いられる場合、第2の用途で用いられる場合の双方において、端末装置と無線通信を行うことにより、端末装置と処理手段との間で非接触式の入出力を行う通信手段とを備えている。

20

【0013】上記第2の目的は、可搬体が電波送信を行っている端末装置に接近した場合、端末装置と可搬体との距離が第1所定距離未満であれば、可搬体が第2の用途に用いられると判定し、端末装置と可搬体との距離が第2所定距離以上第3所定距離以内であれば、可搬体が第1の用途に用いられると判定する判定部を前記特定手段に備えさせることにより達成される。

30

【0014】上記第3の目的は、前記判定部が、前記電波を受信した際の受信電圧が閾値を上回る場合、端末装置と可搬体との距離が第1所定距離未満であると判定し、前記電波を受信した際の受信電圧が閾値を下回る場合、端末装置と可搬体との距離が第2所定距離以上第3所定距離以内であると判定することにより達成される。

【0015】

【発明の実施の形態】集積デバイスを備えた可搬体の一例として、ICカード1を実施する際の実施形態を以下説明する。図1(a)は、実施形態に係るICカード1の外観を示す図であり、図1(b)は、実施形態に係るICカード1の原寸と、その内部構造を示す図である。図1

40

(a)に示すように、本ICカード1は、専用のカードリーダー/ライター100(以下R/W100という)に対して数cm以上10cm以内に接近した場合に、このR/W100と協調処理を行うものである。図1(b)に示すように、ICカード1は、縦53.98mm×横85.60mm×厚み0.76mmであり

(この外寸は、ISO/IEC 7810にて規定されたISOカードサイズに準じている)、所有者は、図1(a)に示すようにこのICカード1を指先で把持することもできる。ICカード1の表面には、所有者の氏名、識別番号を示す文字列を形成した突起部からなるエンボス部(図1(a))

50

中のNo.181319 AAA BBB)が設けられており、図1 (b)に示すように、その内部に4〜5ターンのループアンテナ2と、集積デバイスであるワンチップIC3とを有している。ここで留意すべきは、カード本体の厚みは、僅か0.76mmであり、電池や電源回路をその内部に内蔵することができないという点である。図1 (c)は、ICカードの側面形状を示す拡大図である。図1 (c)からもわかるように、ICカードの側面にはループアンテナ2、ワンチップIC3と電気的な接触を有するコネクタ、ピン等は一切設けられておらず、金属類がICカード外部に全く露出しないようモールドされている。このように、コネクタ、ピン類が一切設けられていないので、ワンチップIC3は、端末装置から電波で供給された電力をループアンテナ2から受け付けることにより、駆動されねばならない。

【0016】続いて、ワンチップIC3の内部構成について説明する。図2は、ワンチップIC3の内部構成を示す図であり、図2に示すように、ワンチップICは、ASK方式復調回路4、コントローラ5、BPSK方式変調回路6、電源再生回路7、スイッチ8、スイッチ9、暗号回路10、暗号回路11、不揮発メモリ12、不揮発メモリ13、及び同期クロック信号発生回路14からなる。

【0017】ASK(Amplitude Shift Keying)方式復調回路4は、ループアンテナ2に誘起した変調波(電波)に対して包絡線検波による復調処理を行って、この変調波の包絡線に重畳されているNRZ(Non-Return-to-Zero)方式のデータをコントローラ5に出力する。ここでASK方式復調回路4により復調される変調波の一例を図3に示す。図3に示すように、ASK方式の変調波は、搬送波の包絡線形状により、“01011101”のデータ列が示されている。また、この変調波は、最大振幅と、最小振幅との比率が約10:9となるASK10%方式と呼ばれる方式にて変調されている。ASK10%では、中心周波数と、データによる周波数とのピーク差が比較的大きいので、端末装置側からの電力供給量を大きくすることができる。更に、この変調波においてデータ列は、106Kbps〜424kbpsの転送レートで、ICカード1に伝送される。この転送レートは、接触型ICカードの転送レートである9600bps(ISO7816 ISO10536に規定されたもの)と比較してかなり高速なので、高速なデータの入出力が可能となり、同じ時間でより大量のデータを処理することが可能となる。

【0018】コントローラ5は、ICカード1におけるモードの管理(1)を行い、不揮発メモリ12、不揮発メモリ13に対するメモリアクセス(2)を行う。コントローラ5により管理されるモード(1)には、端末装置から数cm以上10cm以内の距離内に可搬体が配された場合に稼働されるモード(遠隔モード)と、端末装置の内部回路と前記集積デバイスとの非接触状態を維持しながら可搬体が0mm〜5mmの距離まで端末装置と近接した場合のみ起動されるモード(密接モード)とがある。遠隔モードにお

いてコントローラ5は、不揮発メモリ12に対して出力されるCE1信号をハイレベルに設定し、暗号回路10に対して出力されるSE1信号をハイレベルに設定する。一方、密接モードでは、コントローラ5は、不揮発メモリ12及び不揮発メモリ13に対して出力されるCE2信号をハイレベルに設定し、暗号回路10及び暗号回路11に出力されるSE2信号をハイレベルに設定する。

【0019】コントローラ5によるメモリアクセス(2)とは、ループアンテナ2-ASK方式復調回路4を介して端末装置から出力されたコマンドに従って、不揮発メモリ12、不揮発メモリ13へのデータ書き込みを行うと共に、ループアンテナ2-BPSK方式変調回路6を介して端末装置から出力されたコマンドに従って、不揮発メモリ12、不揮発メモリ13からのデータ読み出しを行って、これをBPSK方式変調回路6-ループアンテナ2に送信させるというものである。密接モードでは、重要な個人情報の入出力が行われることから、端末装置から送信されたデータが暗号化されており、このデータに対する復号又は再暗号化が暗号回路10により行われるので、この復号されたデータ又は再暗号化されたデータを不揮発メモリ12、不揮発メモリ13に書き込む。

【0020】BPSK(Binary Phase Shift Keying)方式変調回路6は、コントローラ5から出力されたデータ列に対してロードスイッチング方式の変調、847.5KHzのサブ搬送波、BPSK方式のサブ変調を行って、第1端末装置に出力する。ここでBPSK方式変調回路6の変調方式は、ASK方式復調回路4とは異なる変調方式なので、BPSK方式変調回路6はASK方式の変調波より電力供給を受けながら、無線出力を行うことができる。

【0021】電源再生回路7は、ASK方式の変調波を整流することにより定電圧を得て、ASK方式復調回路4、コントローラ5、BPSK方式変調回路6、暗号回路10、暗号回路11、不揮発メモリ12、不揮発メモリ13、同期クロック信号発生回路14に供給する。電源再生回路7の内部構成は図4に示されているものである。本図に示すように電源再生回路7は、4つのダイオード、コンデンサを有していて、ループアンテナ2に誘起したASK方式の変調波を整流するダイオードブリッジ回路15と、ダイオードブリッジ回路15からの信号出力を例えば3Vという定電圧に変換する三端子レギュレータ16とからなる。ここでASK方式の変調波にて端末装置から供給を受ける電力は、端末装置との距離の短さに応じて増減する。そのため、このダイオードブリッジ回路15の出力段に現れる電圧は、端末装置との距離が短ければ短い程、大きくなる。このようにASK方式変調波の振幅により変化する電圧は、Vddとしてコントローラ5に出力される。日本国内でICカード1を利用する場合、遠隔モードにおいて電波を介して電源再生回路7により供給される電力は、10mW未満にならざるを得ない。何故なら、日本国内では、電波法という国内法令により、無許可で

10mW以上の出力で電波を送信することは禁じられているからである。これに対して、密接モードにおいて電波を介して供給される電力は、10mW以上にすることが可能である。何故なら、電磁シールドがなされた筐体内でICカード1のループアンテナ2と端末装置のアンテナとを密接させる場合、たとえ、電波法に規制されていたとしても、10mW以上の出力で電波を送信することができるからである。

【0022】スイッチ8は、遠隔モードにおいて解放状態に設定されているが、コントローラ5によりSE2信号がハイレベルに設定された場合のみ、導通状態に設定される。スイッチ8が導通状態に設定されれば、電源再生回路7が発生した定電圧と、同期クロック信号発生回路14が発生した同期クロック信号とが不揮発メモリ13に供給される。

【0023】スイッチ9は、遠隔モードにおいて解放状態に設定されているが、コントローラ5によりSE2信号がハイレベルに設定された場合のみ、導通状態に設定される。スイッチ9が導通状態に設定されれば、電源再生回路7が発生した定電圧と、同期クロック信号発生回路14が発生した同期クロック信号とが暗号回路11に供給される。

【0024】暗号回路10は、ICカード1が端末装置に接近して遠隔モードにてワンチップICが起動され、この端末装置との間で双方向認証を行う際に用いられる。また、密接モードにてワンチップICが起動され、この端末装置との間でセキュリティが強く求められるデータを送受信する際、このデータを暗号化するために用いられる。即ち、電波を復調して得られたデータ列が暗号化されている場合、暗号回路10はこの暗号化データを復号して、コントローラ5に出力する。また、必要に応じて、一旦暗号化されたデータを別の鍵データを用いて再度暗号化してコントローラ5に出力する。暗号回路10による暗号化は、秘密鍵暗号、DES(Data Encryption Standard)暗号、Tr-DES暗号等を用いて行われる。

【0025】暗号回路11は、ICカード1が端末装置に接近して密接モードにて集積デバイスが起動された際、この端末装置との間で双方向認証を行う際に用いられる。この暗号回路11による暗号化は、公開鍵暗号(楕円暗号又はRSA暗号(Rivest, Shamir, Adleman encryption))を用いて行われる。不揮発メモリ12は、約16Byteの記憶容量を有する書込可能な強誘電体メモリ、FeRAM、EEPROMであり、遠隔モードに用いられる個人情報と、密接モードに用いられる個人情報とを記憶しており、CE1信号、CE2信号の何れかが出力された場合に、これらの記憶内容の読み出し/書き込みを行う。

【0026】不揮発メモリ13は、不揮発メモリ12同様、約16Byteの記憶容量を有する書込可能な強誘電体メモリ、FeRAM、EEPROMであり、密接モードのみに用いられる個人情報を記憶しており、CE2信号が出力された場合

に、これらの記憶内容の読み出し/書き込みを行う。不揮発メモリ12及び不揮発メモリ13による個人情報の記憶は以下のように行われる。図6は、不揮発メモリ12及び不揮発メモリ13による個人情報の記憶の概念を説明するために用いるベン図である。図6のベン図において、部分集合Aは、遠隔モードのみに用いられる個人情報の集合であり、部分集合Bは、密接モードのみに用いられる個人情報の集合、部分集合Cは、遠隔モード・密接モードの双方で用いられる個人情報を示す。このような集合において、不揮発メモリ12は、部分集合A・部分集合Cを記憶し、不揮発メモリ13は、部分集合Bを記憶するのである。

【0027】ここでICカード1が金融機関が発行する口座利用者カードである場合、部分集合Cには、残高を割り当てる。部分集合Bには、強い機密性が要求される高額な決済金額、部分集合Aには、処理の利便性が要求される小額な決済金額が割り当てられる。またICカード1が地方自治体が発行する住民カードである場合、部分集合Cには、本人の名称・住所を割り当てる。部分集合Bには、強い機密性が要求される本人の戸籍や源泉徴収の個人情報、部分集合Aには、処理の利便性が要求されるテニスコート、会議場の予約状況が割り当てられる。

【0028】同期クロック信号発生回路14は、ASK方式の変調波から同期クロック信号を得て、この同期クロック信号をコントローラ5、暗号回路10、暗号回路11、不揮発メモリ12、不揮発メモリ13に供給する。同期クロック信号発生回路14の内部構成は、図5に示されているものであり、ASK方式の変調波の振幅電圧と、所定の閾値電圧との比較を行い、搬送波の周波数 f_1 を有するパルス信号を得るコンパレータ17と、このパルス信号の周波数 f_1 を N/M 倍(N は1以上の整数、 M は2以上の整数であり、 $N \times M$ の関係を満たす)に分周して、同期クロック信号を出力する分周器18とからなる。ここで分周器18による分周比は、コントローラ5が発するSE2信号がロウレベルである場合、分周比 P_1 に設定され、コントローラ5が発するSE2信号がハイレベルである場合、分周比 P_2 ($P_2 > P_1$)に設定される。ここで搬送波の周波数が13.56MHzである場合、分周比 P_1 は、同期クロック信号の周波数 $P_1 \times 13.56\text{MHz}$ が1MHz以内になる値に定められており、分周比 P_2 は、同期クロック信号の周波数 $P_2 \times 13.56\text{MHz}$ が2MHzを上回る値に定められている。

【0029】クロック信号の周波数がこのような値に設定されるのは、同期クロック信号の周波数は、集積デバイスの消費電力に影響するからである。即ち、日本国内でICカード1を利用する場合、遠隔モードにおいて電波を介して供給される電力は10mW未満となるので、同期クロック信号発生回路14による分周により得られる同期クロック信号の周波数も、集積デバイスの消費電力が10mW未満になるような周波数(そのような周波数が上記の1MHz以内の周波数である)にせざるを得ない。逆に密接モ

ードにおいて電波を介して供給される電力は10mW以上となるので、同期クロック信号発生回路14による分周により得られる同期クロック信号の周波数を、集積デバイスの消費電力が10mW以上になるような周波数(そのような周波数が上記の2MHz以上の周波数である)に設定することができる。このように密接モードでは、遠隔モードと比較して2倍の周波数の同期クロック信号が供給されるので、集積デバイスは2倍以上の速度で動作することが可能となる。

【0030】続いて、コントローラ5の内部構成について説明する。図7は、コントローラ5の内部構成を示す図である。本図においてコントローラ5は、電圧比較回路19と、メモリ制御部20と、暗号制御部21と、MPU22と、OR回路23と、OR回路24と、OR回路25と、OR回路26とからなる。電圧比較回路19は、ダイオードブリッジ回路15の出力段の電圧Vddと、閾値4Vとの高低比較を行い、ICカード1の動作モードを、密接モード-遠隔モードの何れかに設定する。前記高低比較においてダイオードブリッジ回路15の出力段側のVddの方が高ければ、密接モードであるものとして、SEL信号をハイレベルに立ち上げ、閾値側が高ければ、遠隔モードであるものとして、SEL信号をロウレベルに維持する。

【0031】メモリ制御部20は、MPU22の指示に従って、不揮発メモリ12-不揮発メモリ13のアドレス制御を行うアドレス生成部27と、不揮発メモリ12-不揮発メモリ13からのデータ読み出し及び不揮発メモリ12-不揮発メモリ13へのデータ書き込みを制御するデータ制御部28と、イネーブル信号生成部29とからなる。図8(a)は、イネーブル信号生成部29の内部構成を示す図である。本図において切換信号CEとは、遠隔モード-密接モードのモード切り換えを、MPU22自ら行うのではなく、電圧比較回路19に委ねる場合にハイレベルに設定される信号であり、MPU22が遠隔モード-密接モードのモード切り換えを、自ら行う場合にロウレベルに設定される信号である。

【0032】このようにモード切り換えを、MPU22自ら行うのは以下の場合である。電圧比較回路19によるモード切り換えでは、ICカードが端末装置以外の電波を受けており、ダイオードブリッジ回路15における電圧Vddがたまたま高くなる場合に、誤って密接モードに切り換えられてしまう可能性がある。そのような誤ったモード切り換えが予想される場合、MPU22はコマンドに従ったモード切り換えを行うのである。ここで切換信号CE、Vdd、閾値の組み合わせにより、CE1信号及びCE2信号がどのように選択されるかは図8(b)に表形式で示されている。イネーブル信号生成部29は、電圧比較回路19が出力したSEL信号と、切換信号CEとのAND演算を行い、SEL信号及び切換信号CEの双方がハイレベルならば、不揮発メモリ12及び不揮発メモリ13を選択する

よう、CE2信号をハイレベルに設定するAND回路30と(図8(b)の密接モードの欄参照)、電圧比較回路19が出力したSEL信号の反転値と、切換信号CEとのAND演算を行い、SEL信号がロウレベルであり、切換信号CEがハイレベルならば、不揮発メモリ12のみを選択するよう、CE1信号をハイレベルに設定するAND回路31と(図8(b)の遠隔モードの欄参照)からなる。

【0033】暗号制御部21は、メモリ制御部20の指示に従って、暗号回路10-暗号回路11からのデータ入力及び暗号回路10-暗号回路11へのデータ出力を制御するデータ制御部33と、選択信号生成部34とからなる。図9(a)は、選択信号生成部34の内部構成を示す図である。また、切換信号CE、Vdd、閾値4Vの組み合わせにより、SE1信号及びSE2信号がどのように選択されるかは図9(b)に表形式で示されている。これらの図からもわかるように、選択信号生成部34は、イネーブル信号生成部29と同一であり、SEL信号及び切換信号CEの双方がハイレベルならば、暗号回路10及び暗号回路11を選択するよう、SE2信号をハイレベルに設定するAND回路35と(図9(b)の密接モードの欄参照)、電圧比較回路19が出力したSEL信号の反転値と、切換信号CEとのAND演算を行い、SEL信号がロウレベルであり、切換信号CEがハイレベルならば、暗号回路10のみを選択するよう、SE1信号をハイレベルに設定するAND回路36と(図9(b)の遠隔モードの欄参照)からなる。

【0034】MPU22は、図10に示す内部構成を有しており、モード切り換えを電圧比較回路19に委ねるか自身が行うかを示すフラグを記憶するフラグ記憶部37と、モード切り換えを電圧比較回路19に委ねる場合、切換信号CEをハイレベルに設定し、モード切り換えを自身が行う場合、切換信号CEをロウレベルに設定する切換信号出力部38と、BPSK方式変調回路6からNRZ方式のデータ列が出力されれば、これをコマンドとして取り込むコマンドバッファ39と、コマンドとして取り込まれたデータ列を解析するコマンド解析部40と、解析結果に応じたメモリアクセスを行うメモリアクセス部41と、フラグがモード切り換えを行うものと設定されており、モード切り換えを行う旨が設定されている場合にSE1信号、SE2信号を出力する選択信号生成部42aと、上記コマンドに、モード切り換えを行う旨が設定されている場合にCE1信号、CE2信号を出力するイネーブル信号生成部42bとからなる。コマンドを用いてモード切り換えを行うか、電力を用いてモード切り換えを行うかは、ICカード1の製造業者が出荷時に決定される。また、モード切り換えに用いられるコマンドとは、後述する第1端末装置、第2端末装置がポーリングを行うために発行するポーリングコマンドである。

【0035】以降、図10の構成要素のうち、選択信号生成部42a、イネーブル信号生成部42bについて説

明する。選択信号生成部42aは、コマンドにおいて4bitを占めるアクセス指定フィールドと、4bitを占める暗号指定フィールドとに応じて、SE1信号、SE2信号の出力を制御する。図11(a)は、選択信号生成部42aの内部構成を示す図である。本図の上段は、ポーリングコマンドにおいて4bitを占めるアクセス指定フィールドと、4bitを占める暗号指定フィールドとが示されている。アクセス指定フィールドと、4bitを占める暗号指定フィールドとの組み合わせに応じて、どのようなデータリードが行われるか、データライトが行われるか、SE1信号、SE2信号の何れがハイレベルになるかは図11(b)に示す通りである。

【0036】AND回路43は、暗号指定フィールドの下位2ビットが“00”であり、上位2ビットが“11”であるなら、AND回路46及びAND回路47に“1”を出力する。AND回路44は、アクセス指定フィールドの下位3ビットが“000”であり、上位1ビットが“1”であるなら、AND回路46に“1”を出力する。AND回路45は、アクセス指定フィールドの上位2ビットが“01”であり、下位2ビットが“00”であるなら、AND回路47に“1”を出力する。

【0037】AND回路46は、AND回路43が“1”を出力し、且つ、AND回路44が“1”を出力した場合に、SE1信号を“1”、即ち、ハイレベルに設定する。AND回路47は、AND回路43が“1”を出力し、且つ、AND回路45が“1”を出力した場合に、SE2信号を“1”、即ち、ハイレベルに設定する。以上のような出力を行うことにより、暗号回路10及び暗号回路11は、図11(b)に示すように選択されることになる。

【0038】即ち、暗号指定フィールドが12h(=1100)であり、アクセス指定フィールドが8h(=1000)である場合、SE1信号がハイレベルになって暗号回路10が選択され、暗号指定フィールドが12h(=1100)であり、アクセス指定フィールドが4h(=0100)である場合、SE2信号がハイレベルになって暗号回路10及び暗号回路11が選択されることになる。

【0039】イネーブル信号生成部42bは、ポーリングコマンドにおいて4bitを占めるアクセス指定フィールドと、4bitを占める暗号指定フィールドとに応じて、CE1信号、CE2信号を出力する回路であり、図12(a)に示すように、選択信号生成部42aと同一回路で構成される。また、アクセス指定フィールドと、暗号指定フィールドとの組み合わせに応じて、どのようなデータリードが行われるか、データライトが行われるか、CE1信号、CE2信号の何れがハイレベルになるかは図12

(b)に示されている。アクセス指定フィールドが8h(=1000)である場合、CE1信号がハイレベルに設定されて、不揮発メモリ12及び不揮発メモリ13が選択され、アクセス指定フィールドが4h(=0100)である場合、CE2信号がハイレベルに設定されて不揮発メモリ12のみが選択されることになる。

【0040】以上でMPU22の説明を終え、続いてコントローラ5の残りの構成要素について説明する。図7におけるOR回路23は、MPU22により出力されるCE1信号、イネーブル信号生成部29により出力されるCE1信号の何れか一方を不揮発メモリ12に出力する。OR回路24は、MPU22により出力されるCE2信号、イネーブル信号生成部29により出力されるCE2信号の何れか一方を不揮発メモリ13に出力する。

【0041】OR回路25は、MPU22により出力されるSE1信号、選択信号生成部34により出力されるSE1信号の何れか一方を、不揮発メモリ12に出力する。OR回路26は、MPU22により出力されるSE2信号、選択信号生成部34により出力されるSE2信号の何れか一方を、不揮発メモリ13に出力する。以上で、ICカード1についての説明を終え、続いて、第1端末装置についての説明を開始する。図13は、第1端末装置が備え付けられた自動改札機48を示す図である。自動改札機48は、第1端末装置の制御に従って、開閉される入門ゲート49と、R/W100とが取り付けられている。

【0042】図14は、第1端末装置に設けられているR/W100(以下R/W100を第1端末装置と同一物として説明する)の内部構成を示す図であり、本図において、第1端末装置は電源回路50、インターフェイス装置51、ASK方式変調回路52、BPSK方式復調回路53、コントローラ55、暗号回路56からなる。図14を参照すると、ICカード1には、電源回路が備えられていないのに対して、第1端末装置は、電源回路50を備えていることがわかる。またICカード1は、端末装置から電力供給がなされなければ集積デバイスは稼動することとはなかったが、第1端末装置は、内蔵されている電源回路50にて、常時内部回路が駆動されている。更にICカード1には、他の装置と接続を行うためのインターフェイス装置が一切備えられていなかったが、第1端末装置は、駅の管理システムのホスト装置等との協調処理を行わねばならないので、インターフェイス装置51が備えられている。

【0043】ICカード1は、ASK方式の復調回路と、BPSK方式の変調回路とを備えているのに対して、第1端末装置には、ASK方式の変調回路52と、BPSK方式の復調回路53とが備えられている。ASK方式の変調波は、上述したように多くの電源回路を供給することができるので、第1端末装置はASK方式の変調方式を行うことにより、電源回路が発生した電力を、第1端末装置に接近してくるICカード1に供給するのである。また、ICカード1は秘密鍵を用いて暗号化を行う暗号回路10、公開鍵を用いて暗号化を行う暗号回路11を備えていたのに対して、第1端末装置は、秘密鍵を用いて暗号化を行う暗号回路56のみを備えており、公開鍵を用いて暗号化を行う暗号化回路は備えていない。

【0044】図16は、第1端末装置におけるコントロ

ーラ55と、ICカード1におけるコントローラ5とにより行われる通信プロトコルを示す図である。図16を参照しながら、以降この通信プロトコルについて説明を行う。第1端末装置側のコントローラ55は、ステップS1においてポーリングコマンドを発行していると共に、ステップS2において、ICカード1から発行せられる特定のID番号の受信待ちを行っている。これらステップS1-ステップS2の処理を繰り返し行うことにより、第1端末装置側のコントローラ55は、ICカード1の接近を待機している。ここで図15に示すようにICカードの所有者がICカード1をポケットから取り出して、第1端末装置に接近し、R/W100（第1端末）にICカード1をかざしたものとする。R/W100にかざされれば、ICカード1は、第1端末装置からの電力供給を受けて起動し、ICカード1側コントローラ5は、ステップS3に移行して、第1端末装置から発行せられるポーリングコマンドの受信待ち状態となる。この受信待ち状態において、第1端末装置からポーリングコマンドが発行せれると、ICカード1側のコントローラ5は、ステップS4において特定のID番号を送信する。このように特定のID番号が送信されると、これの受信を待っていた第1端末装置側のコントローラ55の状態は、ステップS2からステップS6に移行する。

【0045】一方、ICカード1側のコントローラ5は、特定ID番号の送信後、密接モードで起動するか、遠隔モードで起動するかの判定を行う。ここでは遠隔モードで起動すると判定されて、ステップS7に移行する。ステップS6及びステップS7は、秘密鍵を用いた相互認証処理を行うステップであり、もし相互認証処理が不正終了すれば、第1端末装置側のコントローラ55は、ステップS8において入門ゲート49を閉ざして、不正カードの所有の疑いがある旨をシステム管理者に通知する。

【0046】続いて、第1端末装置と、ICカードとの間の相互認証について、図17を参照しながら説明する。図17は、第1端末装置と、ICカードとの間で行われる相互認証を示すシーケンス図である。先ず始めに第1端末装置側が主体となった相互認証を行う。先ずステップS51において、第1端末装置におけるコントローラ55は、ID番号を確認する。もしID番号が正当なら、第1端末装置側コントローラ55は、ステップS52において第1端末装置内で乱数を生成して、数値Aに対して予め与えられた秘密鍵Laを用いて暗号化した後、ステップS53において、暗号化により得られた数値VAをICカードに送付する。

【0047】ステップS54において、ICカードのコントローラ5は、第1端末装置からの値VAの受信待ちになっている。ここで、第1端末装置から値VAが送信されると、ステップS55において第1端末装置から予め与えられた秘密鍵Lbを用いて第1端末装置から送信された値VAの復号化を行う。その後、ステップS56において、

復号により得られた数値Bを第1端末装置側に送信する。

【0048】一方、第1端末装置は、ステップS57において、ICカードから送信される数値Bの受信待ちになっており、ICカードから送信されたデータを受信すれば、ステップS57からステップS59に移行する。ステップS59では、受け取ったデータBと、Aとが一致するか否かの判定を行い、一致すればLa=Lbが成立したものと、秘密鍵の相互認証を終えたことになる。もし一致すれば第1端末装置側が主体となった相互認証を終える。

【0049】以降、同様の手順で、ICカード側が主体となった相互認証をステップS60、ステップS61において行う。即ち、ICカードは、数値B以外に乱数値Jを生成し、暗号化して、暗号化された数値VJを第1端末装置に送信して、第1端末装置からこれを復号した数値Kが送信されると、これが数値Jと一致するか否かを判定する。一致しないなら、相互認証処理を不正終了するが、一致するなら、ステップS62において、確認コマンドを第1端末装置に出力して処理を終える。

【0050】ステップS63において、第1端末装置側のコントローラ55は、ICカードからの確認コマンドの受信待ち状態になっており、ステップS63において、ICカードからの確認コマンドを受信すれば、相互認証を終える。相互認証が正常終了すれば、ICカード1側のコントローラ5は図16のステップS9においてリードコマンドの発行待ちとなり、第1端末装置側のコントローラ55は、ステップS10において、不揮発メモリ12に記憶されている乗車区間や定期乗車の有効期間を読み出すよう、第1端末装置側のコントローラ55はリードコマンドを発行し、ステップS11において読み出されたデータの受信待ちとなる。リードコマンドが発行されると、ICカード1側のコントローラ5はステップS9からステップS12に移行し、ステップS12においてリードコマンドの解析及び実行を行った後、不揮発メモリ12及び不揮発メモリ13から乗車区間や定期乗車の有効期間のデータを読み出して、ステップS13においてこれらのデータを第1端末装置に送信し、その後、ステップS14においてライトコマンドの発行待ちとなる。読み出されたデータを受信すると、第1端末装置側のコントローラ55は、ICカード1から読み出された乗車区間や定期乗車の有効期間を参照して、所有者の乗車を許可するか拒否するかを判定する。第1端末装置が設置されている改札が乗車区間外である場合、又は、定期乗車の有効期間が既に終了している場合、第1端末装置側のコントローラ55は、入門ゲート49を閉じて、所有者の搭乗を拒否する。所有者の乗車を許可する場合、ステップS15において第1端末装置側のコントローラ55はライトコマンドを発行し、ステップS16においてデータ書込完了通知の待ち状態となる。

【0051】ライトコマンドが発行されると、ICカード1側のコントローラ5はステップS14からステップS17に移行し、ステップS17においてライトコマンドの解析及び実行を行った後、この所有者が搭乗した旨を不揮発メモリ12に書き込むと共に、ステップS18において、データの書込完了を、第1端末装置に送信する。データ書込の完了が第1端末装置に送信されれば、第1端末装置側のコントローラ5は、ステップS16からステップS1→ステップS2からなるループ状態に移行して、次の所有者の接近を待つ。

【0052】続いて、第2端末装置について説明する。第2端末装置は、現金支払機等、決済用途に用いられるものであり、現金支払い機（キャッシュディスペンサー）として設置されている第2端末装置の一例を図18に示す。本図において、現金支払機60は、ICカード1の挿入口61と、所有者本人の暗証番号、PIN(Personal Identification Number)の入力を受け付けるタッチパネル62と、本人の顔の輪郭或いは肉眼の光彩または指紋等のバイオ情報等をカード所有者から読み取るバイオセンサ63と、カード情報、バイオ情報、ICカード1における相互認証処理により、ICカード1所有者の正当性が確認されたなら、現金支払機60内部の紙幣を機外に送出する紙幣給紙口64とを備える。ここで第2端末装置と、第1端末装置との差違点のうち、最も大きなものは、アンテナの設置箇所である。即ち、第1端末装置は、アンテナを用いて装置外部に電波を放射していたが、第2端末装置は、電波を装置外部に放射するのではなく、装置内部のみで電波を放射させるよう、アンテナを電磁シールドを有した専用ボックスの内部に設けている。

【0053】図19は、アンテナが設けられた専用ボックス65を示す図である。専用ボックス65には、ICカード1を収納するための挿入口61が設けられており、ループアンテナ66と、挿入口61から挿入されたICカード1をループアンテナ66の真下に配置するカードトレイ67と、ICカード1本体にある磁気コード若しくはエンボス等の物理的記録された情報、光学的若しくは光磁気により記録された情報（以下、カード情報と称する）をカードから読み取るカードセンサ68と、収納口62からICカード1を収納して、紙幣給紙口64に装填する装填機構（不図示）とを備えている。図20は、第2端末装置により、ICカード1がどのように上記ループアンテナの真下に挿入されるかを示す図である。本図において、矢印y1に示すように、ICカード1はループアンテナ66の真下に挿入される。このように挿入されると、図21(a)においてループアンテナ66と、ICカード1との間隔は、僅か0mmから5mm程度の密接状態となる。

【0054】このような密接状態で高出力ループアンテナ66に電力が投入されれば、図21(b)の矢印y2、y

3に示すように電波が発生する。ここでループアンテナ66は、その内部から発せられた電波が漏洩しないような電磁シールドを有した専用ボックス65内に備えられているので、ループアンテナ66が、10mwを上回る電力の電波を送信した場合でも、この電波が筐体外部に漏れることはない。日本国内において、10mwより強い電力での送信は、電波法にて禁止されているが、この第2端末装置の内部に設けられたループアンテナは、20mw,30mw等、10mwを上回る電波を用いて、電力を供給することができる。このような大電力の供給により、ICカード1は、密接モードでの動作が可能となる。大電力が供給されれば、ICカード1側の集積デバイスは、高い周波数の同期クロック信号にて動作することが可能であり、その内部のコントローラ5は、高度なアプリケーションプログラムを稼働させることができる。そのようなアプリケーションプログラムには、JAVAカード(JAVAカードとは、SUN-MICRO社が提唱したカード規格である。)向けに開発されたマルチOSソフト、Japan IC Card System Application council(JICSAP)、EMVが提唱するソフトウェア等がある。

【0055】続いて、第2端末装置の内部構成について説明する。図22は、第2端末装置の内部構成を示す図である。図22において、第2端末装置は、電源回路69、インターフェイス装置70、ASK方式変調回路71、BPSK方式復調回路72、コントローラ73、暗号化回路から構成されていて、そのうちASK方式変調回路71、BPSK方式復調回路72は高出力ループアンテナ66と接続しており、カードセンサ68は、コントローラ73と接続している。このうち第2端末装置が第1端末装置と異なるのは、ASK方式変調回路71及びBPSK方式復調回路72が密接モードにて、第1端末装置より大きな電力をICカード1を供給する点と、暗号回路74が、秘密鍵を用いたデータの暗号化、及び、暗号化されたデータの復号を行い、よりセキュリティ性が高い公開鍵暗号を用いて双方向認証を行う点である。

【0056】上記のように構成された第2端末装置の処理内容は、コントローラ73により統合される。図23は、第2端末装置におけるコントローラ73の処理内容を示すフローチャートである。図23を参照しながら、以降この通信プロトコルについて説明を行う。第2端末装置側のコントローラ73は、常時、ステップS21においてカードトレイ67へのICカード1の挿入を待機している。所有者がICカード1を挿入口に挿入すると、ICカード1が第2端末装置内部に収納され、第2端末装置内部にICカード1が装填される。第2端末装置に挿入された状態では、図21(a)に示すように、ICカード1は、第2端末装置側のループアンテナ66と僅かな間隔を空けて密接している。このループアンテナ66の中央付近にICカード1は、配置されるので、ループアンテナ66に電波が誘起すれば、ICカード1は、強力な電力供

給を受けることになる。尚、図21(a)では、ICカードが高出力ループアンテナ66と0~5mmの間隔を空けていたが、この場合でも、ICカードと高出力ループアンテナ66との間の電気的な非接触状態が保たれているのならば、図21(c)に示すように、ICカード1を高出力ループアンテナ66と押し当てても良い。

【0057】ICカード1が装填されると、ステップS22において第2端末装置側のコントローラ73はカードセンサ68に、カード情報の読み取りを行わせ、ステップS23においてカード情報の正当性を認識する。磁気コードやエンボスの欠落や不正に製造された形跡等があり、カード情報の読み取りが正常に行われなかった場合、その旨を所有者に警告して、ICカード1を排出し、ステップS23からステップS29に移行して、不正カードの所有の疑いがある旨をシステム管理者に通知する。カード情報の読み取りが正常に行われた場合、ステップS23からステップS24に移行して暗証番号のキータ입を行うよう提示する。その後、ステップS25において暗証番号のキータ입待ちとなり、暗証番号がキータ입されると、ステップS26においてカード情報に含まれる暗証番号と、キータ입された暗証番号との照合を行う。両者が一致しなかった場合、ICカード1が不正に所有されている疑いがあるものとして、その旨をシステム管理者に通知するようステップS26からステップS29に移行する。両者が一致した場合、ステップS26からステップS27に移行し、バイオセンサ63を起動して、バイオセンサ63に本人の顔の輪郭或いは肉眼の光彩または指紋等のバイオ情報等をICカード1所有者から読み取らせる。そして、ステップS28においてバイオ情報をホスト装置に問い合わせる。ホスト装置には、支給されているICカード1の暗証番号と、バイオ情報とが対応づけたデータベースを有しているので、ホスト装置は、この本人が正当なカード所有者であるかを認識する。もし、バイオセンサ63により読み取られたバイオ情報と、暗証番号との組み合わせがデータベースに存在しないのなら、当該所有者は、そのICカード1を不正に取得したか、或は偽造した疑いがあるので、ステップS28からステップS29に移行して、その旨をシステム管理者に通知する。もし、タッチパネルにより読み取られたバイオ情報と、暗証番号との組み合わせがデータベースに存在するのなら、図24のフローチャートの処理に移行する。

【0058】以降、図24のフローチャートに従って、第2端末装置側のコントローラ73と、ICカード1側のコントローラ5は、協調処理を行う。図24のフローチャートにおいて、図16と同一の参照符号を付したステップは、図16におけるフローチャートと同一であることがわかる。図16と異なるのは、ステップS1においてポーリングコマンドが発行される前に、ステップS31において、高出力ループアンテナ66からの電力供給

が開始する点、ステップS5でのモード切り換えにおいて、密接モードが起動される点、ステップS6-ステップS7において行われていた秘密鍵を用いた相互認証処理が、ステップS32-ステップS33に示す公開鍵を用いた相互認証処理に置き換えられている点、読出コマンド及びライトコマンドを用いてデータの送受信を行う際、このデータが暗号化されており、これの解読を暗号回路10に行わせる点である。また第2端末装置により発行されるポーリングコマンドは、第1端末装置により発行されるポーリングコマンドとは異なるものである。これにより、ICカードは、端末装置に接近する場合又は装填された場合、その端末装置が第1端末装置、第2端末装置の何れであるかを即座に知ることができる。

【0059】続いて、図24のステップS32、ステップS33で行われる第2端末装置と、ICカードとの間の相互認証について、図25を参照しながら説明する。図25は、第2端末装置と、ICカードとの間で行われる相互認証処理を示すシーケンス図である。ステップS71において、第2端末装置側のコントローラ73は、ID番号を確認する。ID番号が正当なら、ステップS72において、第2端末装置内で乱数を生成し、その結果得られた数値Dについてあらかじめ与えられた公開鍵Maと秘密鍵Haのうち公開鍵Maを用いて暗号化した後、暗号化により得られた数値WDをICカードに送付する。

【0060】一方、ICカード側のコントローラ5は、ステップS74において値WDの受信待ち状態になっており、値WDが送信されると、ステップS75において、ICカード側コントローラ5は暗号回路10に予め与えられた公開鍵Mbと秘密鍵Hbのうち秘密鍵Hbを用いて数値WDのデータを復号化を行わせ、復号結果である数値Eを得た後、今度は数値Eに対して公開鍵Mbを用いて暗号化を行い、数値WEを得る。暗号化が行われると、ステップS76において、ICカード側コントローラ5は、暗号化により得られた数値WEを第2端末装置側に送付する。

【0061】第2端末装置側コントローラ73は、ステップS77において、数値WEの受信を待っており、これを受信すれば、ステップS78において第2端末装置側コントローラ73はICカードからのデータWEについて秘密鍵Haで復号化する。その後、第2端末装置側コントローラ73はステップS79において、復号により得られた数値Fが数値Dと一致するか否かを判定する。もし一致すれば第2端末装置側が主体となった相互認証を終える。

【0062】以降、同様の手順で、ICカード側が主体となった相互認証をステップS80、ステップS81において行う。即ち、即ち、ICカードは、数値D以外に乱数値Mを生成し、この数値Mを公開鍵Mbを用いて暗号化して、暗号化された数値WMを第2端末装置に送信する。第2端末装置が、これを秘密鍵を用いて復号した後、公開鍵を用いて暗号化し、その結果得られた数値WNを送信す

る。これが送信されると、これを復号して得られた数値Nと、これが数値Mと一致するか否かを判定する。一致しないなら、相互認証処理を不正終了するが、一致するなら、ステップS82において、確認コマンドを第1端末装置に出力して処理を終える。

【0063】ステップS83において、第2端末装置側のコントローラ55は、ICカードからの確認コマンドの受信待ち状態になっており、ステップS83において、ICカードからの確認コマンドを受信すれば、相互認証を終える。これらのことが行われるので、密接モードでは、遠隔モードによりセキュリティが強く守られることがわかる。

【0064】以上に説明したように本実施形態によれば、第2端末装置側に電磁シールド等、電波が外部に漏洩しないような加工が施されているので、可搬体が端末装置に更に近接して、このような電磁シールドの内部に可搬体が配置されれば、第2端末装置と集積デバイスとの間でかわされる個人情報、悪意の第三者によって不正に傍受されることは無い。また、ICカード1における不揮発メモリ13は、このような近接時にのみ稼働するので、セキュリティが強く求められる個人情報を記憶させれば、ICカード1におけるワンチップICは、端末装置側の内部回路と電気的に接触することなく、セキュリティが強く求められる個人情報の協調処理を第2端末装置との間で行うことができる。このようにICカード1と第2端末装置との協調処理は、集積デバイスと、端末装置側の内部回路との非接触状態を維持したまま行われるので、ICカード1に対しても、第2端末装置に対しても何のメンテナンスも要求されない。加えて、不揮発メモリ13の稼働は端末装置に近接させるだけで行われるので、コネクタの挿抜のような操作が所有者に要求されず、利便性が高いという効果がある。このように本発明のICカード1では、従来の遠隔モードのICカード1同様、遠隔通信による第1端末装置との協調処理を継承しつつも、従来の遠隔モードでは、セキュリティの面から不向きであるとされた金銭決済の用途をも網羅することができるので、個人情報の管理がこの一枚のICカード1に統合されることになる。

【0065】尚、本発明は、その要旨を変更しない範囲で変更実施が可能である。その変更実施の一例には、以下の(a)(b)(c)(d)に示すものがある。

(a) 本実施形態では、第1端末装置が駅の自動改札機に取り付けられたことを想定した説明を行ったが、第1端末装置を現金支払い機(キャッシュディスプレイ)に取り付けて、小額金融を行ってもよい。即ち、この場合、不揮発メモリ12には、所有者の氏名や暗証番号が記憶されている場合、第1端末装置にICカード1が接近すれば、第1端末装置はリードコマンドを発行することにより、これら氏名やPINをICカード1から読み出す。その後、第1端末装置は、融資額を示すライトコマンド

をICカード1に発行する。ICカード1は、このライトコマンドを受信して、不揮発メモリ12にこの融資額を書き込む。その後、第1端末装置は、現金支払い機(キャッシュディスプレイ)に、融資額の支払いを命じる。

【0066】(b) 第1端末を自動改札機、第2端末装置を現金支払い機に設けたが、第1端末装置の機能と、第2端末装置の機能とを備えた端末装置を構成してもよい。即ち、この端末装置は、端末装置から数cm~10cm内にICカードが接近すれば、ワンチップICを遠隔モードに設定させてから、ICカードと電波の送受信を行うことにより、ワンチップICとの間で非接触式の入出力を行い、端末装置から0mm~5mm内にICカードが接近すれば、ワンチップICを密接モードに設定させてから、ICカードと電波の送受信を行うことにより、ワンチップICとの間で非接触式の入出力を行うのである。また、このような機能を汎用コンピュータに行わせるプログラムをコンピュータ読取可能な記録媒体に記録して、利用しても良い。即ち、ここでいう汎用コンピュータは、ASK方式変調回路-BPSK方式復調回路を備えるものであり、上記のようなプログラムは、汎用コンピュータから数cm~10cm内にICカードが接近すれば、ワンチップICを遠隔モードに設定させてから、ICカードと電波の送受信を行うことにより、ワンチップICとの間で非接触式の入出力を行い、汎用コンピュータから0mm~5mm内に可搬体が接近すれば、ワンチップICを密接モードに設定させてから、ICカードと電波の送受信を行うことにより、ワンチップICとの間で非接触式の入出力を行うのである。

【0067】(c) 密接モードへの切り換えは、アンテナにおける受信電圧、ポーリングコマンドを用いて行われたが、ICカード本体の物理的情報、ICカード本体に光学、光磁気を用いて記録された記録情報、ICカード使用者が有する暗証番号、及び、ICカード所有者のバイオ情報の何れか、または、それらの組み合わせと、不揮発メモリに記憶されている個人情報とを用いてモード切り換えを行ってもよい。また、アンテナにおける受信電圧及びポーリングコマンドと、これらを組み合わせてもよい。

【0068】(d) 本実施形態は、MPU22により出力されるCE1,CE2信号と、イネーブル信号生成部29により出力されるCE1,CE2信号の何れか一方を不揮発メモリ12、13に出力したが、MPU22により出力されるCE1,CE2信号と、イネーブル信号生成部29により出力されるCE1,CE2信号の双方が出力された場合のみ、不揮発メモリ12、不揮発メモリ13のメモリアクセスを許可してもよい。このように、双方が出力されたことをモード切り換えの要件とすれば、密接モードへの切り換えが厳密に行われることとなり、ICカードへの不当なアクセスがより困難となる。

【0069】また、MPU22により出力されるSE1,SE2信号と、選択信号生成部34により出力されるSE1,SE2信

号の何れか一方を、暗号回路10、暗号回路11に出力していたが、MPU22により出力されるSE1、SE2信号、選択信号生成部34により出力されるSE1、SE2信号の双方が出力された場合のみ、暗号回路10、暗号回路11を起動しても良い。

【0070】

【発明の効果】 以上説明したように本発明に係る可搬体は、電波送信を行っている端末装置に可搬体が接近すると、可搬体は何れの用途に用いられるかを、端末装置からの電波に基づいて特定する特定手段と、可搬体が第1の用途で用いられる場合には、第1の処理を行い、可搬体が第2の用途で用いられる場合には、第2の処理を行う処理手段と、第1の用途で用いられる場合、第2の用途で用いられる場合の双方において、端末装置と無線通信を行うことにより、端末装置と処理手段との間で非接触式の入出力を行う通信手段とを備えている。

【0071】この可搬体によれば、例えば決済用途と、改札用途とを兼備したコンビネーション型のICカード等、2つの用途で用いられる可搬体を構成する場合、2つの用途の切り換え、及び、端末装置による認識は、端末装置から送信されている電波に基づいて行われることになる。用途切り換え、及び、端末装置による認識が行われる際に、コネクタの挿抜のような操作が所有者に要求されることが無いので本発明の可搬体は利便性が高くなるという効果がある。

【0072】また第1の用途と、第2の用途とにおいて、それぞれ別々の処理が必要となる場合でも、本発明の可搬体において端末装置との入出力は、第1の用途、第2の用途の双方において無線通信にて行われるので、コネクタの接続を行う必要はない。このように用途の切り換えを行う際も、データの入出力を行う際もコネクタ接続が不要となるので、コネクタの磨耗や接触不良を危惧する必要が一切無くなる。よって、可搬体に対しても、端末装置に対しても何のメンテナンスも要求されることが無くなり、決済業務、改札業務の運営が経済的に行われる。

【0073】更に、本発明の可搬体が汚れたり、水に濡れたりしても、それにより、端末装置との通信が行えなくなるようなことはなく、少々乱雑に扱われても、本発明の可搬体は、正常に動作するので、カード所有者は、可搬体の所持及び保管に何の心理的負担も感じないという効果がある。加えて、上記可搬体をISO14443に規定された遠隔型のICカードとして実現する場合、第1の用途、第2の用途の双方において、可搬体は106Kbps～424kbpsの転送レートでデータの入出力を行うことができる。106Kbps～424kbpsという転送レートは、接触型ICカードの転送レートである9600bps(ISO7816 ISO10536に規定されたもの)と比較してかなり高速なので、高速なデータの入出力が可能となり、同じ時間でより大量のデータを処理することが可能となる。

【0074】ここで上記可搬体において、可搬体が電波送信を行っている端末装置に接近した場合、端末装置と可搬体との距離が第1所定距離未満であれば、可搬体が第2の用途に用いられると判定し、端末装置と可搬体との距離が第2所定距離以上第3所定距離以内であれば、可搬体が第1の用途に用いられると判定する判定部を前記特定手段に備えさせてもよい。

【0075】この可搬体によれば、可搬体を端末装置に近づければ可搬体に第2の用途を行わせ、可搬体を端末装置から遠ざければ可搬体に第1の用途を行わせることができるので、端末装置との遠近に応じて、用途の切り換えを行うことができ、所有者は、用途の切り換えが手軽になる。ここで上記可搬体において、前記判定部が、前記電波を受信した際の受信電圧が閾値を上回る場合、端末装置と可搬体との距離が第1所定距離未満であると判定し、前記電波を受信した際の受信電圧が閾値を下回る場合、端末装置と可搬体との距離が第2所定距離以上第3所定距離以内であると判定させてもよい。この可搬体によれば、集積デバイスが電力供給を受けながら稼働する場合、供給可能な電力量に応じて、何れの用途を行うべきかを切り換えるので、第1の処理の処理負荷と、第2の処理の処理負荷とが異なり、それぞれの電力消費量が異なる場合、供給可能な電力に応じて、用途の切り換えを行うことができる。即ち、決済用途では、改札用途と比較して、高い機密性が求められるので、より安全性が高い相互認証を行ったり、また、伝送すべきデータを全て暗号化しておく必要ため、自ずと処理負荷が大きくなるが、可搬体が第1所定距離以内にある場合、端末装置から供給される電力は、極めて大きくなるので、決済用途に必要な機密性が高い処理を行うことが可能となる。

【0076】更に、集積デバイスは端末装置から電力供給を受けて、稼働するので、可搬体内部に電池等を内蔵する必要はない。よって、可搬体の構造を軽薄且つ単純化することができる。ここで前記端末装置には、第1所定電力未満の電波を出力する第1端末装置と、電磁シールドがなされた筐体内部にアンテナを有しており、この筐体内部において、第1所定電力の倍以上の第2所定電力を有する電波を可搬体に出力する第2端末装置とがあり、前記閾値は、前記第2所定距離以上第3所定距離以内の範囲において、第1所定電力の電波を受信した際の受信電力と、当該アンテナから第1所定距離未満の範囲において、第2所定電力の電波を受信した際の受信電力とに基づいて、設定されていてもよい。この場合、第2端末装置側には電磁シールド等、電波が外部に漏洩しないような加工が施されており、可搬体が端末装置に更に近接して、このような電磁シールドの内部に可搬体が配置されるので、端末装置と集積デバイスとの間でかわされる個人情報、悪意の第三者によって不正に傍受されることは無い。このような近接時にのみ行われる第2処

理が、セキュリティが強く求められる個人情報についての処理であれば、集積デバイスは、端末装置側の内部回路と電気的に接触することなく、セキュリティが強く求められる個人情報の協調処理を端末装置との間で行うことができる。従来の遠隔モードのICカード同様、遠隔通信による端末装置との協調処理を継承しつつも、従来の遠隔モードでは、セキュリティの面から不向きであるとされた金銭決済の用途をも網羅することができるので、個人情報の管理がこの一枚の可搬体に統合されることになる。

【0077】また、第1端末装置により供給される電力は、低く抑えることができるので、電力供給するために用いられる電波出力が電波法等の国内法令で規制されている場合であっても、このような法令に違反せずに、端末装置との協調処理を行うことができる。また、端末装置との協調処理は、電波法において国内法令を規制をクリアしているので、端末装置と可搬体との間に必要な通信距離を確保することができる。

【0078】第2の用途は、第1の用途より高い機密性が求められるものであり、第1処理は、第1暗号鍵を用いてデータを暗号化する暗号化処理、第1暗号鍵を用いて暗号化されたデータを復号する復号化処理、端末装置からの認証処理に対して第1暗号鍵を用いて自身の正当性を証明する証明処理、第1暗号鍵を用いて端末装置の正当性を認証する認証処理の何れか1つを含んでいて、第2処理は、前記第1暗号鍵より安全性が高い第2暗号鍵を用いて、データを暗号化する暗号化処理、第2暗号鍵を用いて暗号化されたデータを復号する復号化処理、端末装置からの認証処理に対して自身の正当性を第2暗号鍵を用いて証明する証明処理、第2暗号鍵を用いて端末装置の正当性を認証する認証処理のうち何れか1つを含んでおり、第2処理は、第1処理より処理負荷が大きく、前記第2所定電力は、処理手段が第2処理を行う場合に消費される電力に基づいた値に設定されている。この可搬体によれば、高い機密性が求められる第2の用途では、安全性が高い暗号鍵が用いられるので、従来の遠隔モードのICカード同様、遠隔通信による端末装置との協調処理を継承しつつも、従来の遠隔モードでは、セキュリティの面から不向きであるとされた金銭決済の用途をも網羅することができるので、個人情報の管理がこの一枚の可搬体に統合されることになる。

【0079】ここで前記集積デバイスは、第1の用途においてのみ用いられるデータを記憶する第1領域と、第2の用途のみにおいて用いられるデータを記憶する第2領域を含む記憶手段を含み、前記通信手段は、端末装置から無線にて発行されたコマンドを受信すると共に、端末装置に出力すべきデータを無線にて端末装置に送信する送受信部を備え、前記処理手段は、特定手段により何れかの用途が特定された場合、第1領域及び第2領域のうち、特定された用途に割り当てられている領域のみの

アクセスを許可し、それ以外の領域のアクセスを禁止するアクセス管理部と、前記送受信部が受信したコマンドを解読する解読部と、前記解読部による解読結果がリードコマンドである場合、リードコマンドにて指示されているデータを第1領域又は第2領域から読み出して、送受信部に送信させ、解読結果がライトコマンドである場合、ライトコマンドにて指示されたデータを第1領域又は第2領域に書き込むメモリアクセス部とを含んでいてもよい。この可搬体によれば、特定された用途に割り当てられている領域のみのアクセスを許可し、それ以外の領域のアクセスを禁止するので、第2領域において、機密性が強く求められる個人情報が記憶されているとしても、この可搬体が通常に携帯されている状態において、悪意の第三者による電波を用いた不正な読み出しは不可能となる。

【0080】ここで前記集積デバイスは、第1端末装置から第1所定電力が供給された場合、受信信号における搬送波の周波数に基づいた第1周波数を有する同期クロック信号を処理手段に供給すると共に、第2端末装置から第2所定電力が供給された場合、第1周波数より高い第2周波数を有する同期クロック信号を処理手段に供給する同期クロック信号発生部を備えていてもよい。この可搬体によれば、供給電力が大きくなった場合に、同期クロック信号の周波数を高くするので、集積デバイスの高速動作が可能となる。高い周波数の同期クロック信号にて、第2回路が稼働されるので、JAVAカード等のマルチOSソフトの適用が可能となる。

【0081】ここで可搬体と通信を行う端末装置であって、可搬体には、集積デバイスが設けられており、前記集積デバイスは、所定の処理を行う第1モード、第1モードよりも機密性が高い処理を行う第2モードの何れかに設定され、端末装置は、その内部にアンテナを有しており、アンテナから放射された電波が一定値以上装置外部に放射されないように電磁シールドがなされている筐体と、この筐体内部に可搬体が挿入されると、集積デバイスを第2モードに設定させてから、アンテナに電波を放射させることにより、集積デバイスとの通信を行う通信手段とを備えていてもよい。端末装置には電磁シールド等、電波が外部に漏洩しないような加工が施されており、可搬体が端末装置に更に近接して、このような電磁シールドの内部に可搬体が配置されるので、端末装置と集積デバイスとの間でかわされる個人情報が、悪意の第三者によって不正に傍受されることは無い。このような近接時にのみ行われる第2モードが、セキュリティが強く求められる個人情報についての処理であれば、集積デバイスは、端末装置側の内部回路と電気的に接触することなく、セキュリティが強く求められる個人情報の協調処理を端末装置との間で行うことができる。従来の遠隔モードのICカード同様、遠隔通信による端末装置との協調処理を継承しつつも、従来の遠隔モードでは、セキュ

リティの面から不向きであるとされた金銭決済の用途をも網羅することができるので、個人情報の管理がこの一枚の可搬体に統合されることになる。

【0082】前記端末装置は、この筐体内部に可搬体が挿入されると、可搬体の正当性を物理的に示す物理情報を可搬体から読み取る第1読み取り部と、所有者本人の正当性を示す所有者情報の入力を所有者から受け付ける受付部と、所有者本人の肉体的な特徴を示すバイオ情報を所有者から読み取る第2読み取り部のうち、少なくとも1つを備えており、前記通信手段は、第1読み取り部が読み取った物理個人情報、受付部が受け付けた所有者情報、第2読み取り部が読み取ったバイオ情報のうち、少なくとも1つを用いて、所有者又は可搬体の正当性を確認してから、集積デバイスの状態を第2モードに設定させてもよい。この端末装置によれば、可搬体の正当性を物理的に示す物理情報、所有者本人の正当性を示す所有者情報、所有者本人の肉体的な特徴を示すバイオ情報の組み合わせで、可搬体及び所有者の認証の正当性を高度に確認することが可能となり、偽造に対する防止策を確固たるものにすることができる。

【図面の簡単な説明】

【図1】(a)実施形態に係るICカード1の外観を示す図である

(b)実施形態に係るICカード1の原寸と、その内部構造を示す図である。

(c)ICカードの側面形状を示す拡大図である。

【図2】ワンチップIC3の内部構成を示す図である。

【図3】ASK方式の変調波を示す図である。

【図4】電源再生回路7の内部構成を示す図である。

【図5】同期クロック信号発生回路14の内部構成を示す図である。

【図6】不揮発メモリ12及び不揮発メモリ13による個人情報の記憶の概念を説明するために用いるベン図である。

【図7】コントローラ5の内部構成を示す図である。

【図8】(a)イネーブル信号生成部29の内部構成を示す図である。

(b)イネーブル信号生成部29による出力を表形式で示す図である。

【図9】(a)選択信号生成部34の内部構成を示す図である。

(b)選択信号生成部34による出力を表形式で示す図である。

【図10】現金支払機60の内部構成を示す図である。

【図11】(a)選択信号生成部42aの内部構成を示す図である。

(b)選択信号生成部42aによる出力を表形式で示す図である。

【図12】(a)イネーブル信号生成部42bの内部構成を示す図である。

(b)イネーブル信号生成部42bによる出力を表形式で示す図である。

【図13】第1端末装置が備え付けられた自動改札機48を示す図である。

【図14】第1端末装置の内部構成を示す図である。

【図15】所有者がICカード1をポケットから取り出して、第1端末装置に接近し、第1端末装置のアンテナにICカード1をかざした様子を示す図である。

【図16】第1端末装置におけるコントローラ55と、ICカード1におけるコントローラ5とにより行われる通信プロトコルを示す図である。

【図17】第1端末装置と、ICカードとの間で行われる相互認証を示すシーケンス図である。

【図18】現金支払い機(キャッシュディスペンサー)として設置されている第2端末装置の一例を示す図である。

【図19】ループアンテナが設けられた専用ボックス65を示す図である。

【図20】第2端末装置により、ICカード1がどのように上記ループアンテナの真下に挿入されるかを示す図である。

【図21】(a)ICカード1が第2端末装置側のループアンテナ66と僅かな間隔を空けて密接している状態を示す図である。

(b)ICカード1が第2端末装置側のループアンテナ66と僅かな間隔を空けて密接している状態において矢印y2,y3に示すように電波が発生している様子を示す図である。

(c)ICカード1を高出力ループアンテナ66と押し当てるように第2端末装置に装填した図である。

【図22】第2端末装置の内部構成を示す図である。

【図23】第2端末装置におけるコントローラ73の処理内容を示すフローチャートである。

【図24】第2端末装置側のコントローラ73と、ICカード1側のコントローラ7と協調処理を行う様子を示す図である。

【図25】第1端末装置と、ICカードとの間で行われる相互認証を示すシーケンス図である。

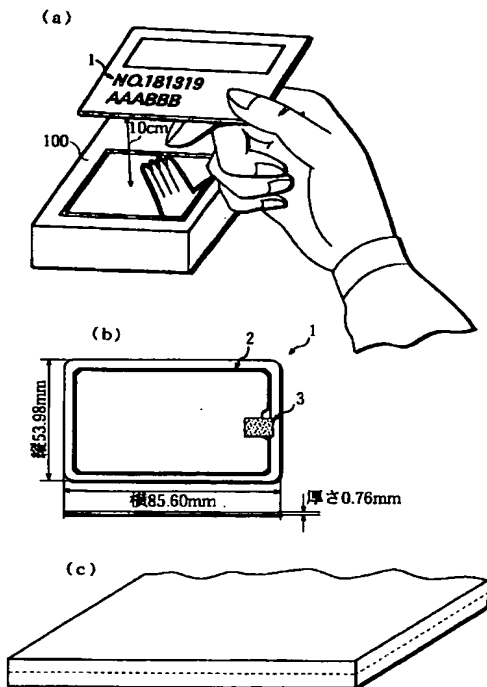
【符号の説明】

- 2 ループアンテナ
- 4 ASK方式復調回路
- 5 カード側コントローラ
- 6 BPSK方式変調回路
- 7 電源再生回路
- 8 スイッチ
- 9 スイッチ
- 10 暗号回路
- 11 暗号回路
- 12 不揮発メモリ
- 13 不揮発メモリ

31

- 14 同期クロック信号発生回路
- 15 ダイオードブリッジ回路
- 16 三端子レギュレータ
- 17 コンパレータ
- 18 分周器
- 19 電圧比較回路
- 48 自動改札機
- 49 入門ゲート
- 50 電源回路
- 51 インターフェイス装置
- 55 端末装置側コントローラ
- 56 暗号回路
- 60 現金支払機

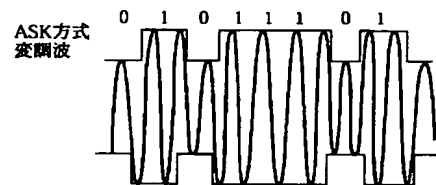
【図1】



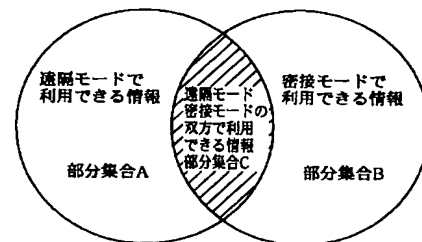
32

- 61 挿入口
- 62 タッチパネル
- 62 収納口
- 63 バイオセンサ
- 64 紙幣給紙口
- 65 専用ボックス
- 66 高出力ループアンテナ
- 67 カードトレイ
- 68 カードセンサ
- 10 73 端末装置側コントローラ
- 74 暗号化回路
- 100 カードリーダー/ライター

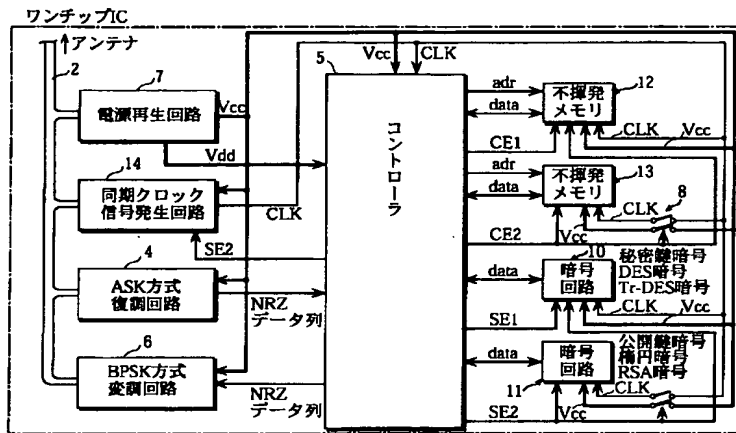
【図3】



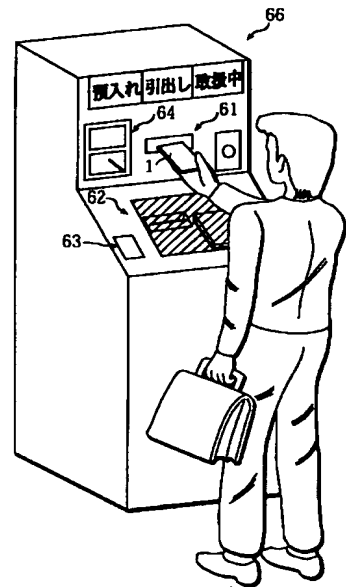
【図6】



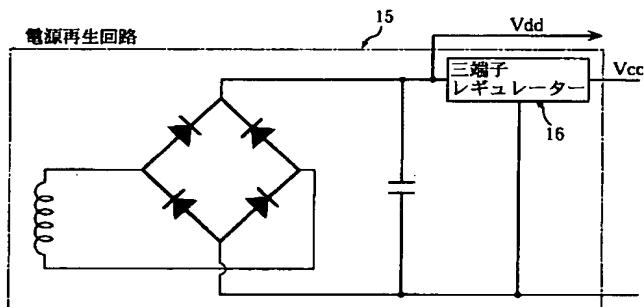
【図2】



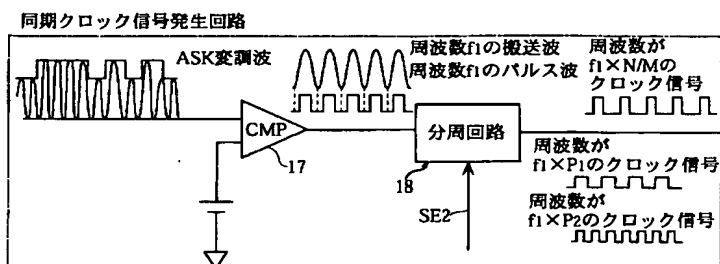
【図18】



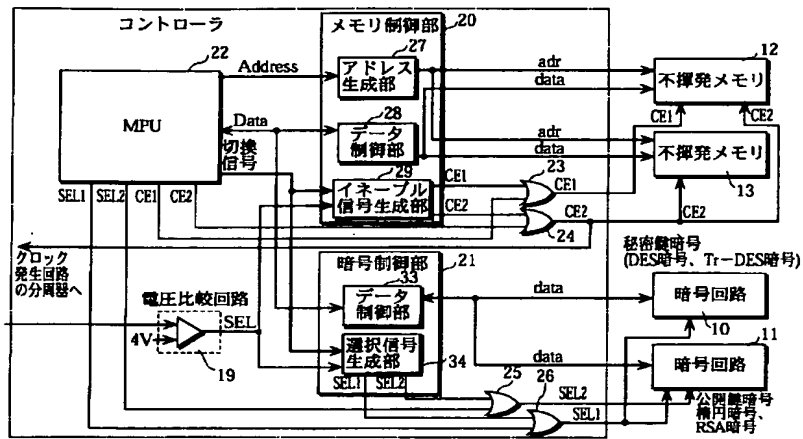
【図4】



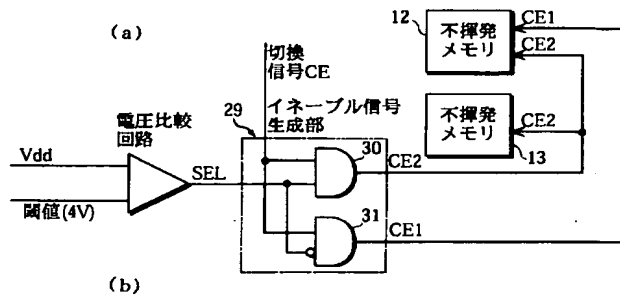
【図5】



【図7】

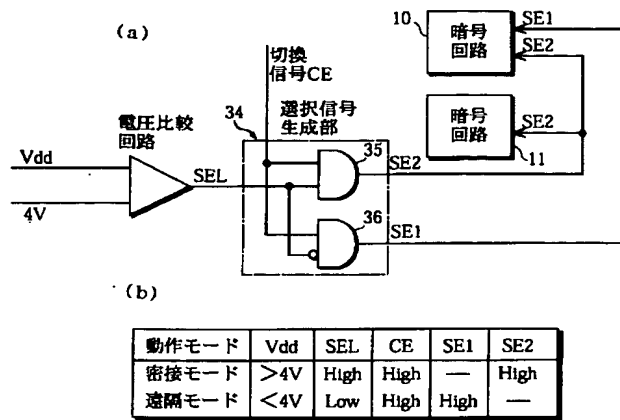


【図8】

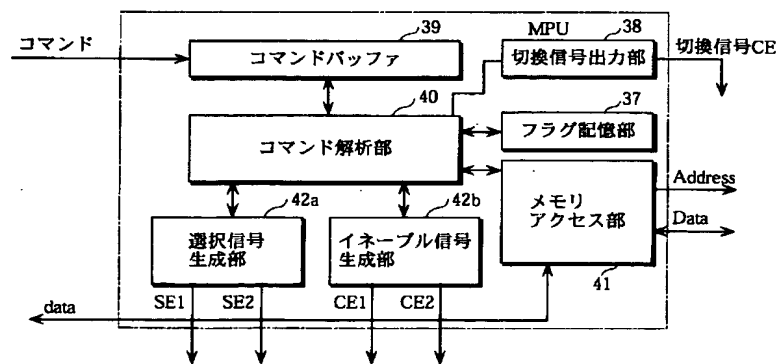


動作モード	Vdd	SEL	CE	CE1	CE2
密接モード	>4V	High	High	—	High
遠隔モード	<4V	Low	High	High	—

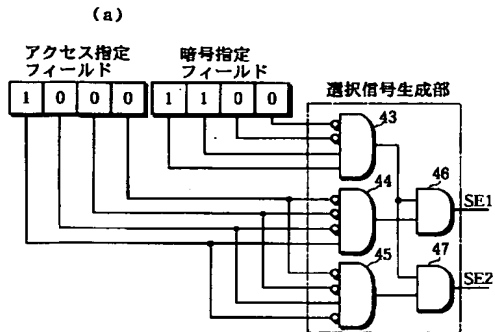
【図9】



【図10】



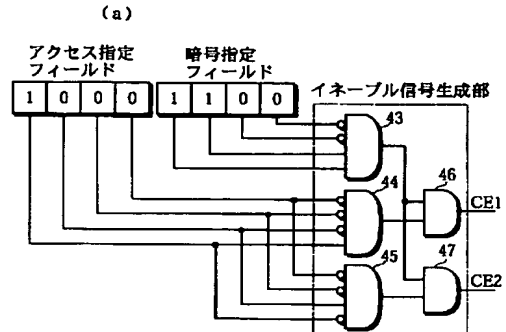
【図11】



(b)

略号指定	アクセス指定	説明
8h	—	リード
4h	—	ライト
12h	8h	SE1
	4h	SE2

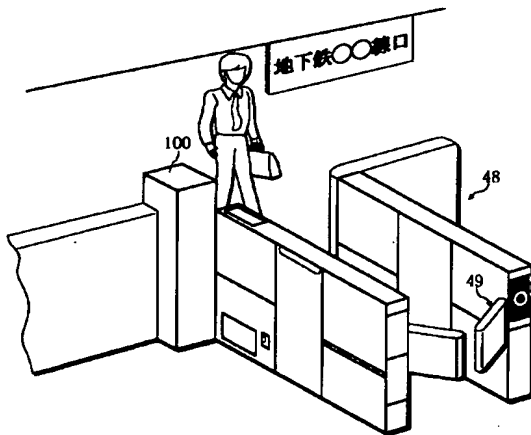
【図12】



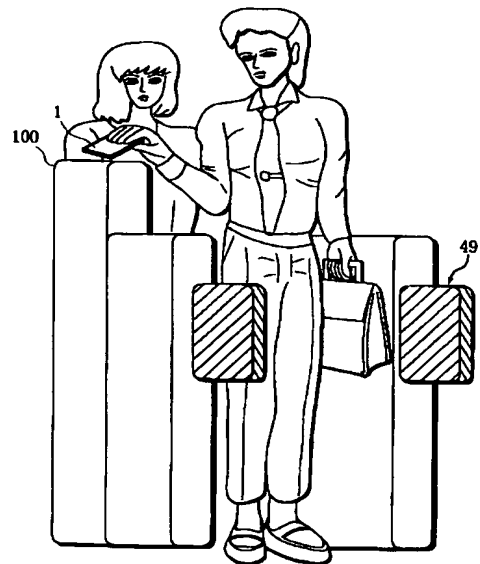
(b)

略号指定	アクセス指定	説明
8h	—	リード
4h	—	ライト
12h	8h	CE1
	4h	CE2

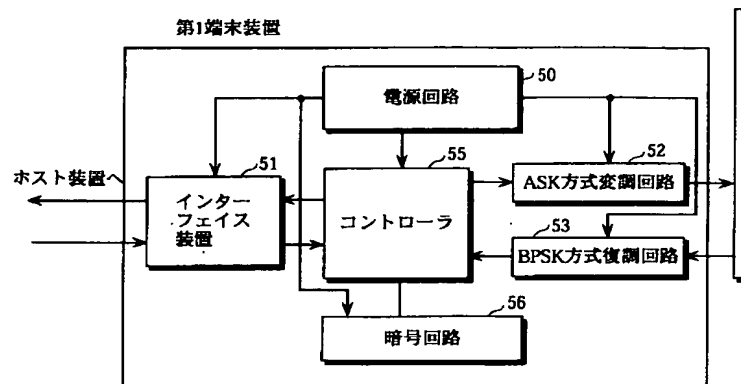
【図13】



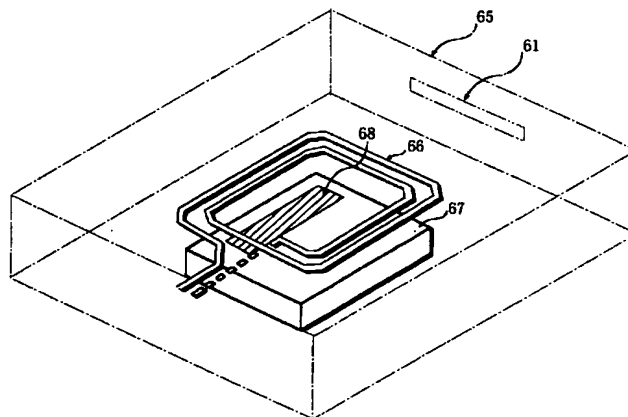
【図15】



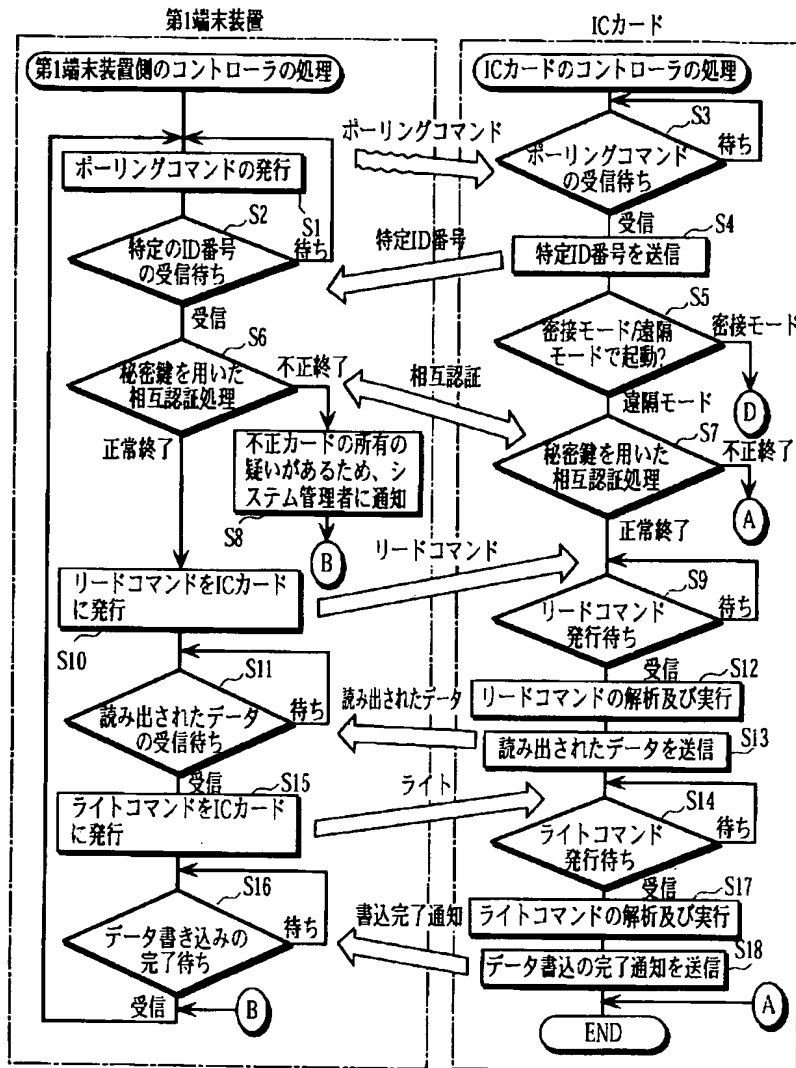
【図14】



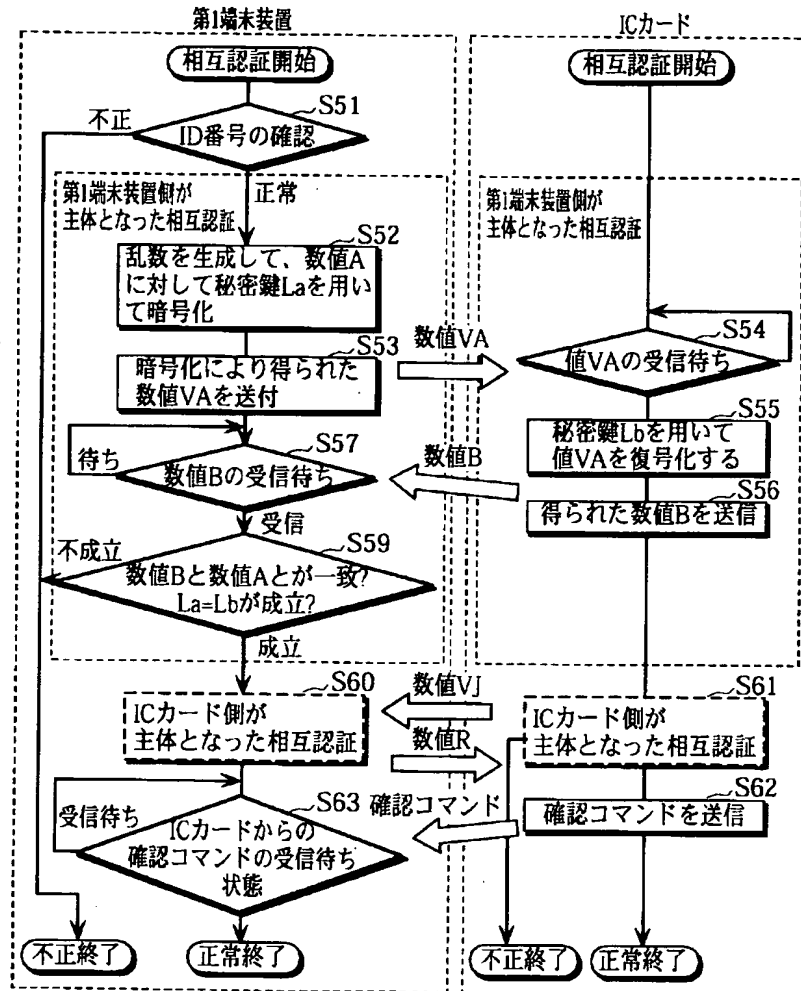
【図19】



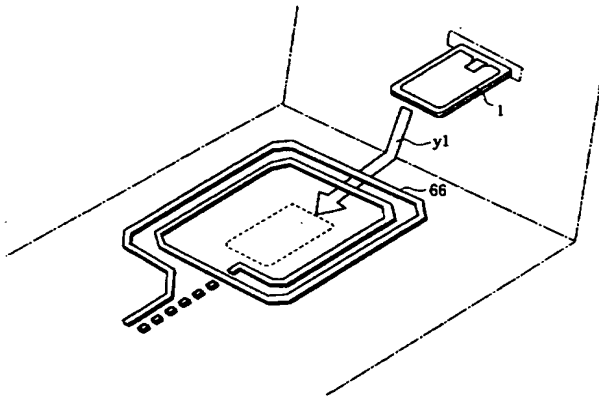
【図16】



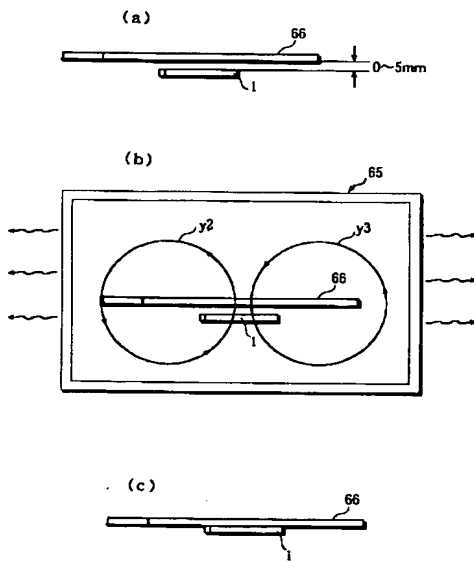
【図17】



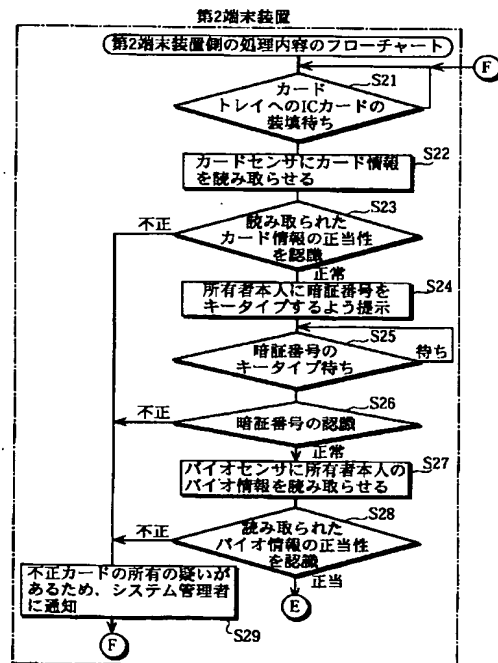
【図20】



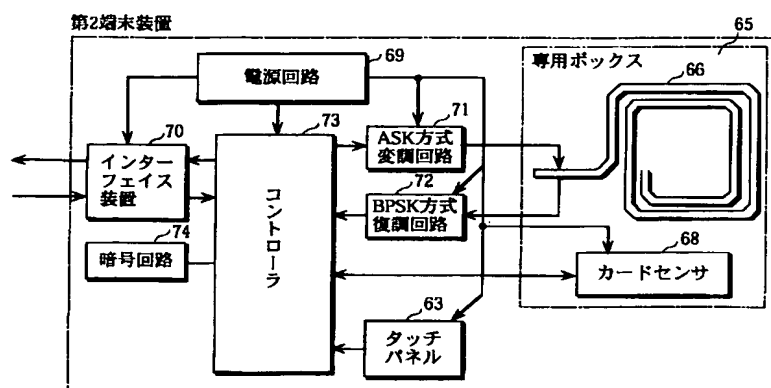
【図21】



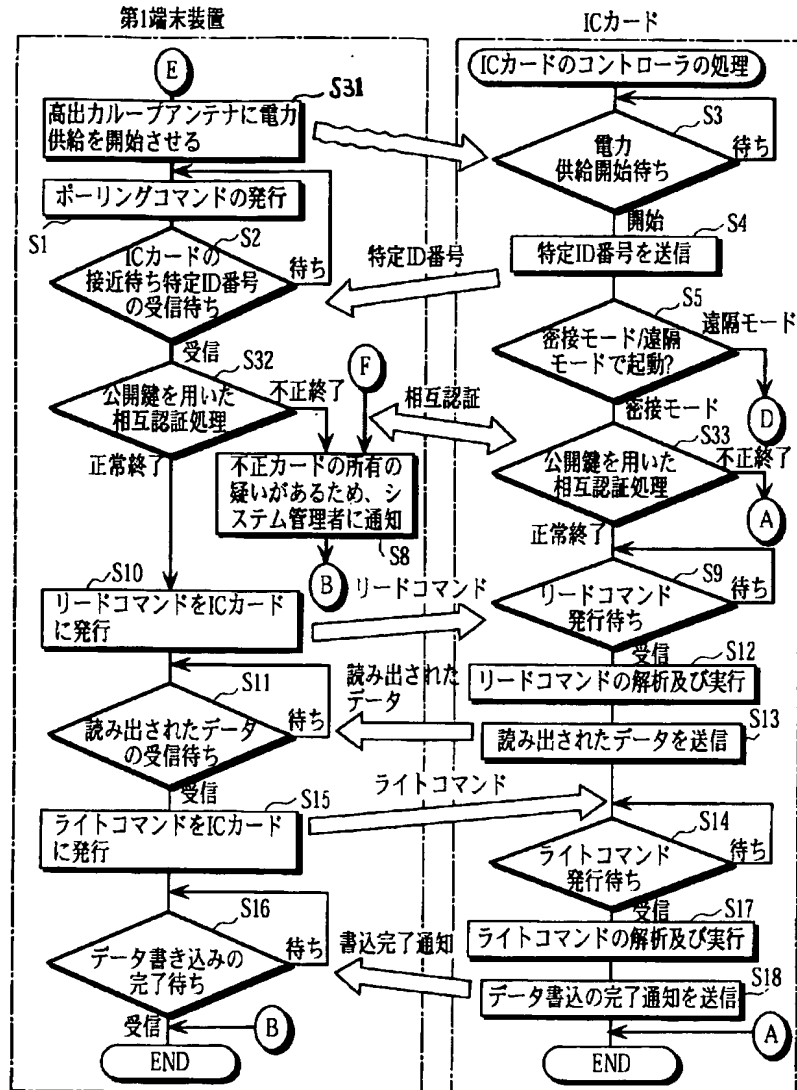
【図23】



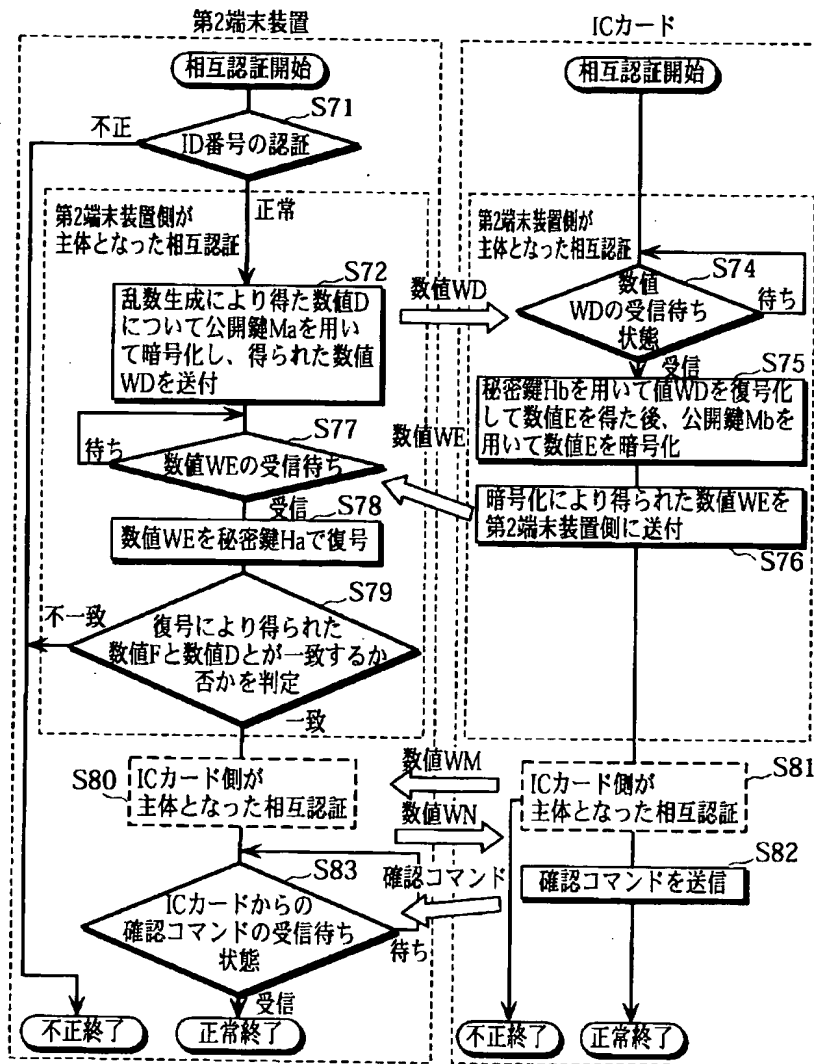
【図22】



【図24】



【図25】



フロントページの続き

(51)Int.Cl.⁷

H04L 9/32

識別記号

FI

H04L 9/00

テーマコード(参考)

675B